ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η\Υ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΔΙΚΤΥΩΝ

"Διαχείριση συστημάτων αισθητήρων βασιζόμενα σε τεχνολογία RFID"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αγγελική Τσολή

***Επιβλέποντες καθηγητές*:**
Λέανδρος Τασιούλας
Ιορδάνης Κουτσόπουλος

Βόλος, Ιούλιος 2005

UNIVERSITY OF THESSALY
Department of Computer & Communications Engineering

"Sensor-based management systems based on RFID technology"

DIPLOMA THESIS

Angeliki Tsoli

***Advisors*:**
Leandros Tassiulas
Iordanis Koutsopoulos

Volos, July 2005

Contents

Figures

Acknowledgements

I would like to thank professor Leandros Tassiulas who has guided me throughout my thesis as well as lecturer Iordanis Koutsopoulos for his remarks that helped me trigger my imagination.

Last but not least, I would like to thank my family who has supported me throughout all these years.

Abstract

In this diploma thesis, the RFID technology is analyzed (operating principles, readers' and tags' hardware, coding, modulation, anticollision procedures, frequencies, standards, applications). Moreover, a protocol to synchronize readers working in a multi-reader multi-tag environment is proposed. The protocol is applied to the store shelf scanning application and further refined to meet the requirements of this specific application.

1. Introduction

1.1 Automatic Identification

In recent years, automatic identification procedures (Auto ID) have become very popular in many service industries, manufacturing companies and material flow systems. Automatic identification procedures exist to provide information about people, animals, goods and products.

The omnipresent barcode labels that triggered a revolution in identification systems some considerable time ago are being found to be inadequate in an increasing number of cases. Barcodes may be extremely cheap, but their stumbling block is their low storage capacity and the fact that they cannot be reprogrammed.

The technically optimal solution would be the storage of data in a silicon chip. The most common form of electronic data carrying device in use in everyday life is the chip card based upon a contact field (telephone chip card, bank cards). However, the mechanical contact used in the chip card is often impractical. A contactless transfer of data between the data carrying device and its reader is far more flexible. In the ideal case, the power required to operate the electronic data carrying device would also be transferred from the reader using contactless technology. Because of the procedures used for the transfer of power and data, contactless ID systems are called RFID (Radio Frequency Identification) systems.

1.2 Radio Frequency Identification

Radio Frequency Identification (RFID) is a technology that provides wireless identification and tracking capability that is more robust than that of a bar code and, therefore, offers the capability to significantly improve supply chain management efficiency, including lower labour costs, higher inventory velocity and improved market intelligence. RFID, which was developed during WW II, first appeared commercially in the early 1980s. The technology has historically been used for niche applications, primarily closed loop, high-end asset tracking. A lack of standards, relatively high cost and other barriers have prevented broad-based adoption. However, it is expected that the requirements imposed by Wal-Mart and the U.S. Department of Defense on their supplier base will reduce these barriers and lead to greater use of RFID in the broader supply chain market during the next decade.

1.2.1 RFID System Components

An RFID system is made up of two components:

- A **reader** (or **interrogator,** or, sometimes, **base station**), including an **antenna**:

The device that is used to read and/or write data to RFID tags.

A reader typically contains a radio frequency module (transmitter and receiver), a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface (RS 232, RS 485, etc.) to enable them to forward the data received to another system (PC, robot control system, etc.)

- A **tag** (or **transponder**), including an **antenna**:

The device that is located on the object to be identified and transmits data to a reader.

The transponder, which represents the actual data-carrying device of an RFID system, normally consists of a coupling element and an electronic microchip. When the transponder, which does not usually possess its own voltage supply (battery), is not within the response range of a reader it is totally passive. The transponder is only activated when it is within the response range of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.

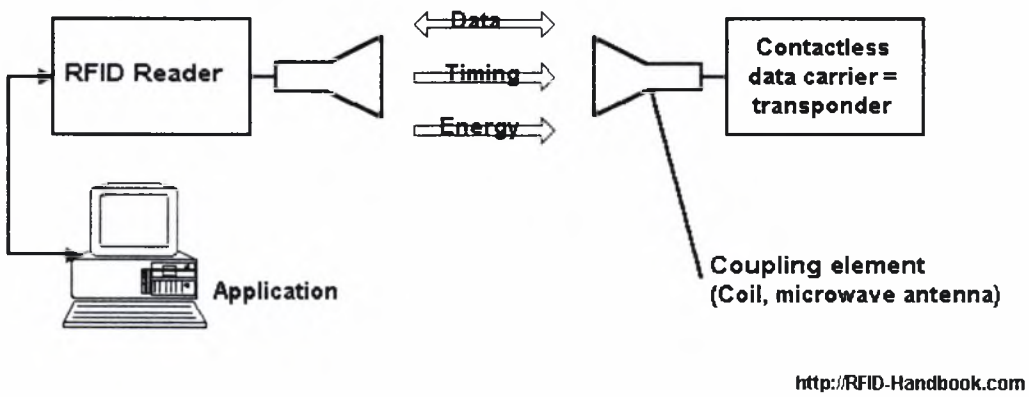

Figure 1.1: The components of an RFID system.

1.2.2 Data flow in an application

A *software application* that is designed to read data from a contactless data carrier (transponder) or write data to a contactless data carrier requires a contactless reader as an interface.

Write and read operations involving contactless data carrier are performed on the basis of the *master-slave principle*. This means that all reader and transponder activities are initiated by the application software. In a hierarchical system structure the application software represents the master, while the reader, as the slave, is only activated when write/read commands are received from the application software.

To execute a command from the application software, the reader first enters into communication with a transponder. The reader now plays the role of the master in relation to the transponder. The transponder therefore only responds to commands from the reader and is never active independently (except for the simplest read-only transponders).

1.3 Bar Codes Vs. RFID

Bar codes are predominately used today for identifying and tracking products throughout the supply chain. Even though they can achieve efficiencies in the order of 90%, they still show some limits in the technology for which RFID is able to provide a better solution and further optimization. The advantages of RFID when compared with bar codes include the following:

- **Simultaneous Identification**

Unlike other Auto ID methods where items must be physically separated or read individually, numerous RFID smart label transponders can be read simultaneously – identifying multiple labels, containers or items all at the same time as they pass a reading location or are read with a handheld scanner. This need is critical in supply chain logistics, especially at the item-tagging level, where there could be 25 different items in a box travelling on a pallet with 30 other boxes passing through a tunnel reader or portal all at the same time. RFID is the only technology that can read individual items simultaneously.

- **Non Line-Of-Sight**

RFID provides a contactless data link without the need for line-of-sight. With this technology, labels can be hidden or embedded in items, but still read. This isn't possible with other Auto ID methods such as bar codes.

- **Data Storage**

RFID can store upwards of 30 times more data than bar codes, allowing the tag to carry a range of real-time information about an item at multiple points in the supply chain. Mass serialization or the ability to store a unique serial number for each and every item is something that cannot be accomplished with bar codes. Tag size is also a factor. To store all the data pharmaceutical companies would like to track at various points in the supply chain would require large bar codes – perhaps larger than the item it's adhered to – or may even require the application of multiple bar codes.

- **Read/Write**

RFID tags act as data carriers. Information can be written to and updated on the tag, which is specific to an item, container or pallet in the supply chain. This information is then held with that item, acting as a travelling item history or self-contained database. Read/write tags could also potentially provide a migration path to the EPC Network once is has been built to support electronic track and trace using networked databases.

- **Read Reliability**

First-pass accuracy is important in supply chain applications. With RFID, the need for spending time scanning items multiple times is eliminated. Using other Auto ID technologies requiring line-of-sight, tags sometimes have to be run through the system a second time or be manually read.

- **Durability**

Without concerns about harsh or dirty environments that restrict other Auto ID technologies, the durability of RFID technology is especially suited to fit the needs of supply chain and warehousing applications. In warehouses where harsh environments are the norm, RFID smart labels can be read through dirt, soiled packaging or other materials.

- **Difficult To Replicate**

While linear or 2-D bar codes can easily be replicated by counterfeiters by simply scanning and printing them, the RFID tag manufacturing process would require a great deal more expertise, investment, and time to copy. Counterfeiters would potentially have to build or have access to a semiconductor wafer fabrication facility in order to manufacture the chips and assemble them to inlays or labels. It would also require significantly more time to replicate the individual EPC serial numbers.

However, RFID does have drawbacks relative to bar coding such as higher cost, incomplete infrastructure and significantly less standardization, which are covered in greater detail in chapter 12 ("Historical Barriers to RFID Adoption").

A brief comparison between barcodes and RFID systems is presented in the following table:

System parameters	Barcodes	RFID systems
Typical data quantity (bytes)	1 - 100	16 – 64 k
Data density	Low	Very high
Machine readability	Good	Good
Readability by people	Limited	Impossible
Influence of dirt/damp	Very high	No influence
Influence of (optical) covering	Total failure	No influence
Influence of direction and position	Low	No influence
Degradation/wear	Limited	No influence

Purchase cost/ reading electronics	Very low	Medium
Operating costs (e.g. printer)	Low	None
Unauthorised copying/ modification	Slight	Impossible
Reading speed (including handling of data carrier)	Low ~ 4 s	Very fast ~ 0.5 s
Maximum distance between data carrier and reader	0 – 50 cm	0 – 5 m

Figure 1.2: Barcodes vs. RFID

2. Operating Principles

The operating principles of the different RFID systems are shown in the following figure and they are analysed in the following sections.

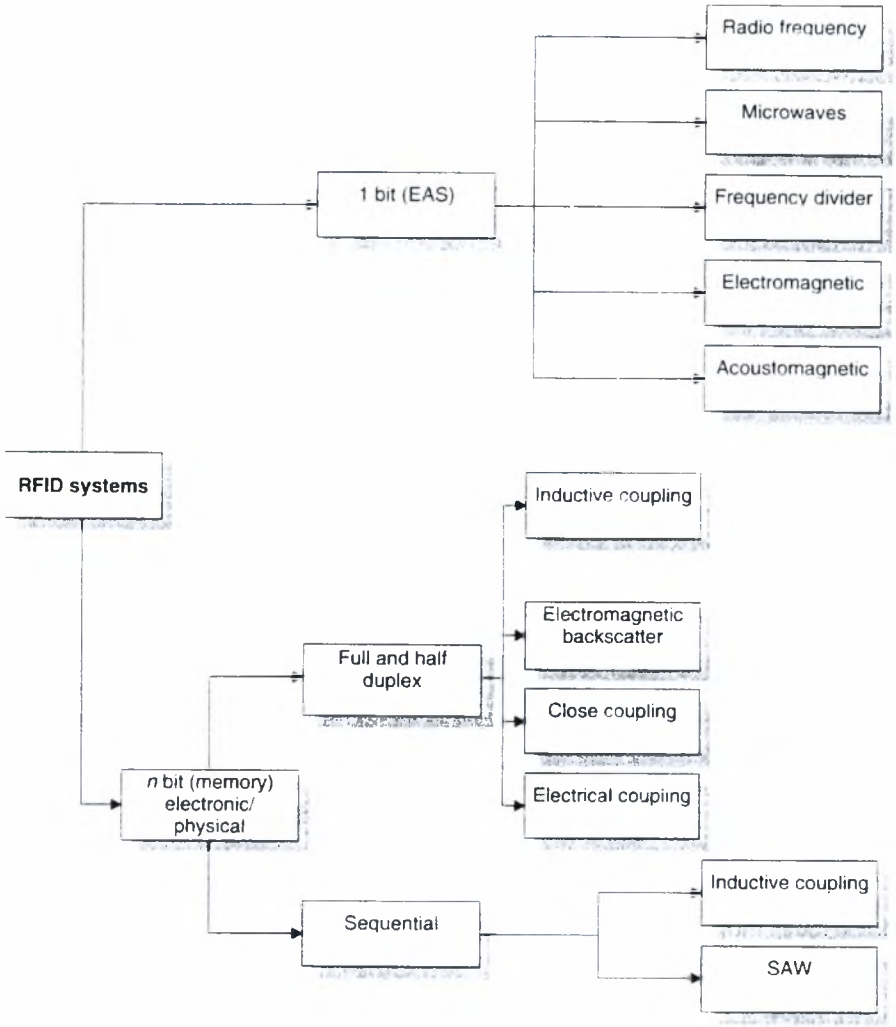

Figure 2.1: The different operating principles of RFID systems.

2.1 1-bit Transponders

A bit is the smallest unit of information that can be represented and has only two states: 1 and 0. This means that only two states can be represented by systems based upon a 1-bit transponder: 'transponder in interrogation zone' and 'no transponder in interrogation zone'. Despite this limitation, 1-bit transponders are very widespread – their main field of application is in electronic anti-theft devices in shops (EAS, electronic article surveillance).

An EAS system is made up of the following components: the antenna of a *reader*, the *security element* or *tag*, and an optional *deactivation device* for deactivating the tag after payment. In modern systems deactivation takes place when the price code is registered at the till. Some systems also incorporate an *activator*, which is used to reactivate the security element after deactivation.

2.1.1 Radio frequency

The *radio frequency (RF) procedure* is based upon LC resonant circuits adjusted to a defined resonant frequency f_R. Early versions employed inductive resistors made of wound enamelled copper wire with a soldered on capacitor in a plastic housing (*hard tag*). Modern systems employ coils etched between foils in the form of stick-on labels. To ensure that the damping resistance does not become too high and reduce the quality of the resonant circuit to an unacceptable level, the thickness of the aluminium conduction tracks on the 25 µm thick *polyethylene foil* must be at least 50 µm. Intermediate foils of 10 µm thickness are used to manufacture the capacitor plates.

The reader (detector) generates a magnetic alternating field in the radio frequency range (***figure 2.2***). If the LC resonant circuit is moved into the vicinity of the magnetic alternating filed, energy from the alternating field can be induced in the resonant circuit via its coils (Faraday's law). If the frequency f_G of the alternating field corresponds with the resonant frequency f_R of the LC resonant circuit, the resonant circuit produces a *sympathetic oscillation*. The current that flows in the resonant circuit as a result of this acts against its cause, i.e. it acts against the external magnetic alternating field. This effect is noticeable as a result of a small change in the voltage drop across the transmitter's generator coil and ultimately leads to a weakening of the measurable magnetic field strength. A change to the induced voltage can also be detected in an optional sensor coil as soon as a resonant oscillating circuit is brought into the magnetic field of the generator coil.

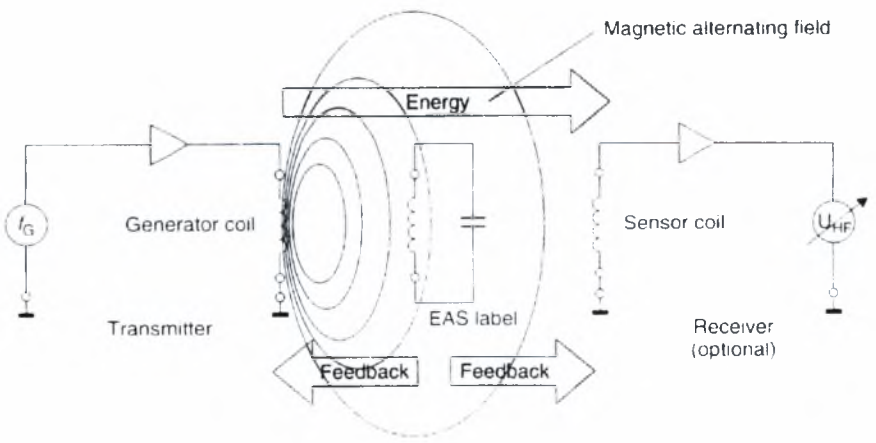

Figure 2.2: Operating principle of the EAS radio frequency procedure.

The relative magnitude of this dip is dependent upon the gap between the two coils (generator coil – security element, security element – sensor coil) and the quality Q of the induced resonant circuit (in the security element).

The relative magnitude of the changes in voltage at the generator and sensor coils is generally very low and thus difficult to detect. However, the signal should be as clear as possible so that the security element can be reliably detected. This is achieved using a bit of a trick: the frequency of the magnetic field generated is not constant, it is 'swept'. This means that the generator frequency continuously crosses the range between minimum and maximum. The frequency range available to the swept systems is 8.2 MHz ± 10%.

Whenever the swept frequency exactly corresponds with the resonant frequency of the resonant circuit (in the transponder), the transponder begins to oscillate, producing a clear dip in the voltages at the generator and sensor coils. Frequency tolerances of the security element, which depend upon manufacturing tolerances and vary in the presence of a metallic environment, no longer play a role as a result of the 'scanning' of the entire frequency range.

Because the tags are not removed at the till, they must be altered so that they do not activate the anti-theft system. To achieve this, the cashier places the protected product into a device – the deactivator – that generates a sufficiently high magnetic field that the induced voltage destroys the foil capacitor of the transponder. The capacitors are designed with intentional short-circuit points, so-called *dimples*. The breakdown of the capacitors is irreversible and detunes the resonant circuit to such a degree that this can no longer be excited by the *sweep signal*.

Large area *frame antennas* are used to generate the required magnetic alternating field in the detection area. The frame antennas are integrated into columns and combined to form gates.

2.1.2 Microwaves

EAS systems in the microwave range exploit the generation of harmonics at components with nonlinear characteristic lines (e.g. diodes). The *harmonic* of a sinusoidal voltage A with a defined frequency f_A is a sinusoidal voltage B, whose frequency f_B is an integer multiple of the frequency f_A. The subharmonics of the frequency f_A are thus the frequencies $2f_A$, $3f_A$, $4f_A$, etc. The Nth multiple of the output frequency is termed the Nth harmonic (Nth harmonic wave); the output frequency itself is termed the carrier wave or fist harmonic.

In principle, every two-terminal network with a nonlinear characteristic generates harmonics at the first harmonic. In the case of *nonlinear resistances*, however, energy is consumed, so that only a small part of the first harmonic power is converted into the harmonic oscillation. Under favourable conditions, the multiplication of f to n x f occurs

with an efficiency of $\eta = 1 / n^2$. However, if nonlinear energy storage is used for multiplication, then in the ideal case there are no losses.

Capacitance diodes are particularly suitable nonlinear energy stores for frequency multiplication. The number and intensity of the harmonics that are generated depend upon the capacitance diode's *dopant profile* and characteristic line gradient. The exponent ***n*** (also γ) is a measure for the gradient (= capacitance-voltage characteristic). For simple diffused diodes, this is 0.33, for alloyed diodes it is 0.5 and for tuner diodes with a hyper-abrupt P-N junction it is around 0.75.

The capacitance-voltage characteristic of alloyed capacitance diodes has a quadratic path and is therefore best suited for the doubling of frequencies. Simple diffused diodes can be used to produce higher harmonics.

The layout of a 1-bit transponder for the generation of harmonics is extremely simple: a capacitance diode is connected to the base of a *dipole* adjusted to the carrier wave (***figure 2.3***). Given a carrier wave frequency of 2.45 GHz the dipole has a total length of 6 cm. The carrier wave frequencies used are 915 MHz (outside Europe), 2.45 GHz or 5.6 GHz. If the transponder is located within the transmitter's range, then the flow of current within the diode generates and re-emits harmonics of the carrier wave. Particularly distinctive signals are obtained at two or three times the carrier wave, depending upon the type of diode used.

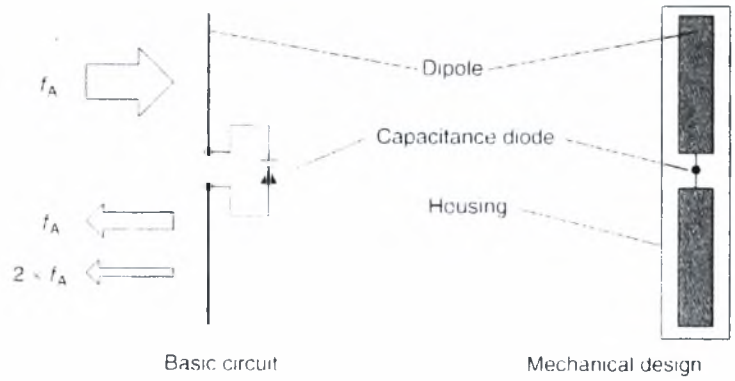

Figure 2.3: Basic circuit and typical construction format of a microwave tag.

2.1.3 Frequency divider

This procedure operates in the long wave range at 100-135 kHz. The security tags contain a semiconductor circuit (microchip) and a resonant circuit coil made of wound enamelled copper. The resonant circuit is made to resonate at the operating frequency of the EAS system using a soldered capacitor. These transponders can be obtained in the form of hard tags (plastic) and are removed when goods are purchased.

The microchip in the transponder receives its power supply from the magnetic field of the security device. The frequency at the self-inductive coil is divided by two by the microchip and sent back to the security device. The signal at half the original frequency is fed by a tap into the resonant circuit coil (***figure 2.4***).

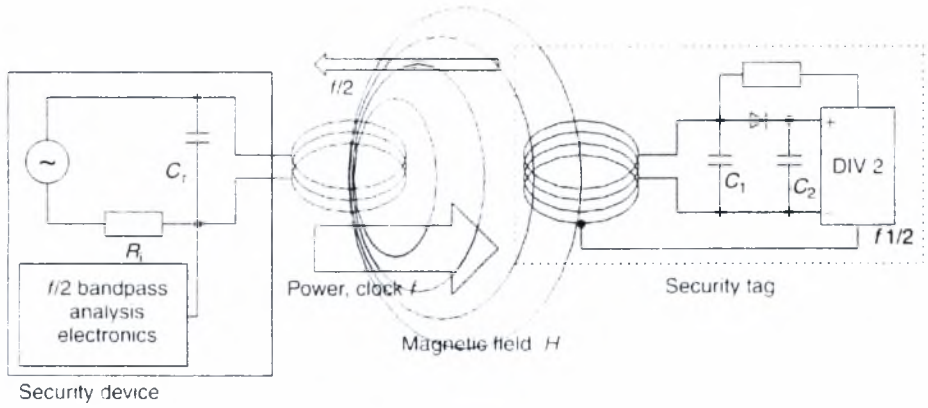

Figure 2.4: Basic circuit diagram of the EAS frequency division procedure: security tag (transponder) and detector (evaluation device).

The magnetic field of the security device is pulsed at a lower frequency (ASK modulated) to improve the detection rate. Similarly to the procedure for the generation of harmonics, the modulation of the carrier wave (ASK or FSK) is maintained at half the frequency (*subharmonic*). This is used to differentiate between 'interference' and 'useful' signals. This system almost entirely rules out false alarms.

Frame antennas are used as sensor antennas.

2.1.4 Electromagnetic types

Electromagnetic types operate using strong magnetic fields in the NF range from 10 Hz to around 20 kHz. The security elements contain soft magnetic amorphous metal strips with a steep flanked hysteresis curve. The magnetisation of these strips is periodically reversed and the strips taken to magnetic saturation by a strong magnetic alternating field. The markedly nonlinear relationship between the applied field strength H and the magnetic flux density B near saturation, plus the sudden change of flux density B in the vicinity of the zero crossover of the applied field strength H, generates harmonics at the basic frequency of the security device, and these harmonics can be received and evaluated by the security device.

The electromagnetic type is optimised by superimposing additional signal sections with higher frequencies over the main signal. The marked nonlinearity of the strip's hysteresis curve generates not only harmonics but also signal sections with summation and differential frequencies of the supplied signals. Given a main signal of frequency f_S = 20

Hz and the additional signals f_1 = 3.5 and f_2 = 5.3 kHz, the following signals are generated (first order):

$$f_1 + f_2 = f_{1+2} = 8.80 \text{ kHz}$$
$$f_1 - f_2 = f_{1-2} = 1.80 \text{ kHz}$$
$$f_s + f_1 = f_{s+1} = 3.52 \text{ kHz}$$

The security device does not react to the harmonic of the basic frequency in this case, but rather to the summation or differential frequency of the extra signals.

The tags are available in the form of self-adhesive strips with lengths ranging from a few centimeters to 20 cm. Due to the extremely low operating frequency, electromagnetic systems are the only systems suitable for products containing metal. However, these systems have the disadvantage that the function of the tags is dependent upon position: for reliable detection the magnetic field lines of the security device must run vertically through the amorphous metal strip.

For deactivation, the tags are coated with a layer of hard magnetic metal or partially covered by hard magnetic plates. At the till the cashier runs a strong *permanent magnet* along the metal strip to deactivate the security elements. This magnetizes the hard magnetic metal plates. The metal strips are designed such that the remanence filed strength of the plate is sufficient to keep the amorphous metal strips at saturation point so that the magnetic alternating field of the security system can no longer be activated.

The tags can be reactivated at any time by demagnetization. The process of deactivation and reactivation can be performed any number of times. For this reason, electromagnetic goods protection systems were originally used mainly in lending libraries. Because the tags are small (min. 32 mm short strips) and cheap, these systems are now being used increasingly in the grocery industry.

In order to achieve the field strength necessary for demagnetization of the permalloy strips, the filed is generated by two coil systems in the columns at either side of a narrow passage. Several individual coils, typically 9 to 12, are located in the two pillars, and these generate weak magnetic fields in the center and stronger magnetic fields on the outside. Gate widths of up to 1.50 m can now be realized using this method, while still achieving detection rates of 70%.

2.1.5 Acoustomagnetic

Acoustomagnetic systems for security elements consist of extremely small plastic boxes around 40 mm long, 8 to 14 mm wide depending upon design, and just a millimetre high. The boxes contain two metal strips, a *hard magnet metal strip* permanently connected to the plastic box, plus a strip made of *amorphous metal*, positioned such that it is free to vibrate mechanically.

Ferromagnetic metals (nickel, iron, etc.) change slightly in length in a magnetic field under the influence of the field strength H. This effect is called magnetostriction and results from a small change in the interatomic distance as a result of magnetisation. In a magnetic alternating field a magnetostrictive metal strip vibrates in the longitudinal direction at the frequency of the field. The amplitude of the vibration is especially high if the frequency of the magnetic alternating field corresponds with that of the (acoustic) resonant frequency of the metal strip. This effect is particularly marked in amorphous materials.

The decisive factor is that the magnetostrictive effect is also reversible. This means that an oscillating magnetostrictive metal strip emits a magnetic alternating field. *Acoustomagnetic security systems* are designed such that the frequency of the magnetic alternating field generated precisely coincides with the resonant frequencies of the metal strips in the security element. The amorphous metal strip begins to oscillate under the influence of the magnetic field. If the magnetic alternating field is switched off after some time, the excited magnetic strip continues to oscillate for a while like a tuning fork and thereby itself generates a magnetic alternating field that can easily be detected by the security system (***figure 2.5***).

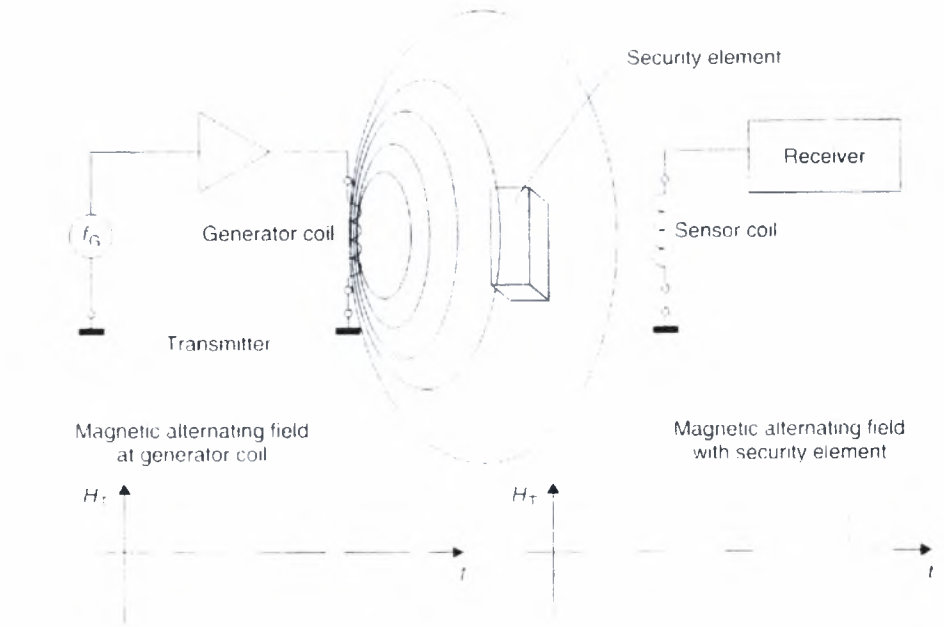

Figure 2.5: Acoustomagnetic system comprising transmitter and detection device (receiver). If a security element is within the field of the generator coil, this oscillates like a tuning fork in time with the pulses of the generator coil. The transient characteristics can be detected by an analyzing unit.

The great advantage of this procedure is that the security system is not itself transmitting while the security element is responding and the detection receiver can thus be designed with a corresponding degree of sensitivity.

In their activated state, acoustomagnetic security elements are magnetised, i.e. the above-mentioned hard magnetic metal strip has high remanence field strength and thus forms a permanent magnet. To deactivate the security element the hard magnetic metal strip must be demagnetised. This detunes the resonant frequency of the amorphous metal strip so it can no longer be excited by the operating frequency of the security system. The hard magnetic metal strip can only be demagnetised by a strong magnetic alternating field with slowly decaying field strength. It is thus absolutely impossible for the security element to be manipulated by permanent magnets brought into the store by customers.

2.2 n-bits Transponders

In contrast to 1-bit transponders, which normally exploit simple physical effects (oscillation stimulation procedures, stimulation of harmonics by diodes or the nonlinear hysteresis curve of metals), the transponders described in this and subsequent sections use an electronic microchip as the data-carrying device. This has a data storage capacity of up to a few kilobytes.

When an RFID tag and reader communicate they share energy and transfer information. Information transfer can take place on the downlink – from the reader to the tag – or on the uplink – from the tag to the reader. RFID systems typically utilize one of three communication procedures to perform this energy sharing and information transfer: full duplex (FDX), half duplex (HDX) and sequential (SEQ).

In the ***half duplex procedure (HDX)***, the data transfer from the transponder to the reader alternates with the data transfer from the reader to the transponder. At frequencies below 30 MHz this is most often used with the load modulation procedure, either with or without a subcarrier, which involves very simple circuitry. Closely related to this is the modulated reflected cross-section procedure that is familiar from the radar technology and is used at frequencies above 100 MHz. Load modulation and modulated reflected cross-section procedures directly influence the magnetic or electromagnetic field generated by the reader and are therefore known as *harmonic* procedures.

In the ***full duplex procedure (FDX)***, the data transfer from tag to reader takes place at the same time as the data transfer from reader to the transponder. This includes procedures in which data is transmitted from the transponder at a fraction of the frequency of the reader, i.e. a subharmonic, or at a completely independent, i.e. an anharmonic, frequency. However, both procedures have in common the fact that the transfer of energy from the reader to the transponder is continuous, i.e. it is independent of the direction of data flow.

In ***sequential systems (SEQ)***, on the other hand, the transfer of energy from the transponder to the reader takes place for a limited period of time only (pulse operation → *pulsed system*). Data transfer from the transponder to the reader occurs in the pauses between the power supply to the transponder.

Figure 2.6: RFID communication procedures

2.3.1 Full and Half Duplex Procedures

2.3.1.1 Inductive Coupling

Power supply to passive transponders

An inductively coupled transponder comprises of an electronic data carrying device, usually a single microchip, and a large area coil, which functions as an antenna.

Inductively coupled transponders are almost always operated passively. This means that all the energy needed for the operation of the microchip has to be provided by the reader. For this purpose, the reader's antenna coil generates a strong, high frequency electro-magnetic field, which penetrates the cross-section of the coil area and the area around the coil. Because the wavelength of the frequency range used (< 135 kHz: 2400 m, 13.56 MHz: 22.1 m) is several times greater than the distance between the reader's antenna and the transponder, the electro-magnetic field may be treated as a simple magnetic alternating field with regard to the distance between transponder and antenna (***figure 2.7***).

A small part of the emitted field penetrates the antenna coil of the transponder, which is some distance away from the coil of the reader. By induction, a voltage U is generated in the transponder's antenna coil. This voltage is rectified and serves as the power supply for the data carrying device (microchip). A capacitor C_1 is connected in parallel with the reader's antenna coil, the capacitance of which is selected such that it combines with the coil inductance of the antenna coil to form a parallel resonant circuit, with a resonant frequency that corresponds with the transmission frequency of the reader. Very high currents are generated in the antenna coil of the reader by resonance step-up in the

parallel resonant circuit, which can be used to generate the required field strengths for the operation of the remote transponder.

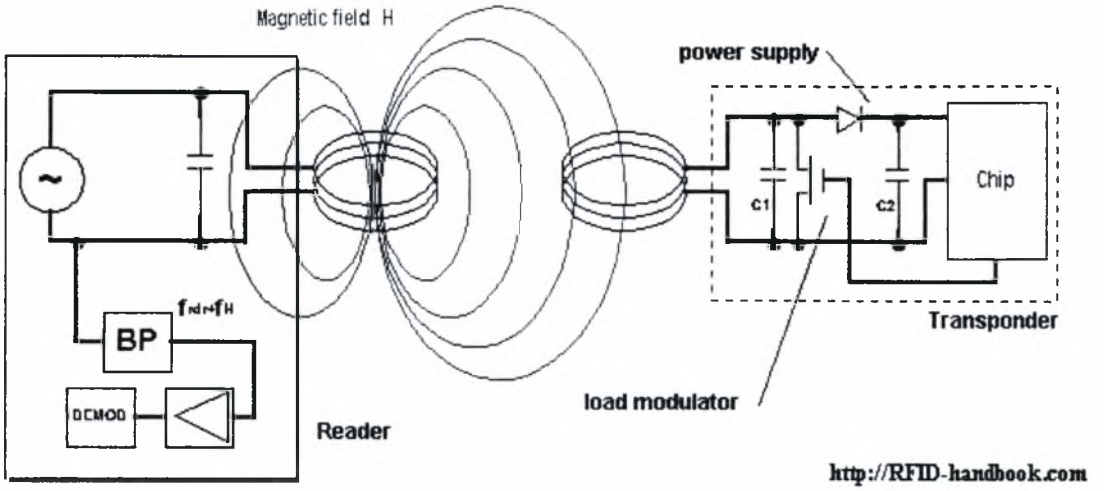

Figure 2.7: Operating principle of an inductive coupling transponder.

The antenna coil of the transponder and the capacitor C_1 are connected to form a resonant circuit tuned to the transmission frequency of the reader. The voltage U at the transponder coil reaches a maximum due to resonance step-up in the parallel resonant circuit.

The layout of the two coils can also be interpreted as a transformer (*transformer coupling*), in which case there is only a very weak coupling between the two windings. The efficiency of power transfer between the antenna coil of the reader and the transponder is proportional to the operating frequency f, the number of windings n, the area A enclosed by the transponder coil, the angle of the two coils relative to each other and the distance between the two coils.

As frequency f increases, the required coil inductance of the transponder coil, and thus the number of windings n decreases (135 kHz: typical 100-1000 windings, 13.56 MHz: typical 3-10 windings). Because the voltage induced in the transponder is still proportional to the frequency f, the reduced number of windings barely affects the efficiency of power transfer at higher frequencies.

Data transfer from transponder to reader

- *Load modulation*

As described above, inductively coupled systems are based upon a *transformer-type coupling* between the primary coil in the reader and the secondary coil in the transponder. This is true when the distance between the coils does not exceed 0.16 λ, so that the transponder is located in the ***near field*** of the transmitter antenna.

If a resonant transponder (i.e. the self-resonant frequency of the transponder corresponds with the transmission frequency of the reader) is placed within the magnetic alternating field of the reader's antenna, then this draws energy from the magnetic field. The resulting feedback of the transponder on the reader's antenna can be represented as *transformed impedance* Z_T in the antenna coil of the reader. Switching a load resistor on and off at the transponder's antenna therefore brings about a change in the impedance Z_T and thus voltage changes at the reader's antenna. This has the effect of an amplitude modulation of the voltage U_L at the reader's antenna coil by the remote transponder. If the timing with which the load resistor is switched on and off is controlled by data, this data can be transferred from the transponder to the reader. This type of data transfer is called ***load modulation***.

To reclaim the data in the reader, the voltage measured at the reader's antenna is rectified. This represents the demodulation of an amplitude modulated signal.

➢ *Load modulation with subcarrier*

Due to the weak coupling between the reader antenna and the transponder antenna, the voltage fluctuations at the antenna of the reader that represent the useful signal are smaller by orders of magnitude than the output voltage of the reader.

In practice, for a 13.56 MHz system, given an antenna voltage of approximately 100 V (voltage step-up by resonance) a useful signal of around 10mV can be expected (=80 dB signal/noise ratio). Because detecting this slight voltage change requires highly complicated circuitry, the modulation sidebands created by the amplitude modulation of the antenna voltage are utilised.

If the additional load resistor in the transponder is switched on and off at a very high elementary frequency f_s, then two spectral lines are created at a distance of $\pm f_s$ around the transmission frequency of the reader f_{READER}, and these can be easily detected (however f_s must be less than f_{READER}). In the terminology of radio technology the new elementary frequency is called a *subcarrier*. Data transfer is by ASK, FSK or PSK modulation of the subcarrier in time with the data flow. This represents an amplitude modulation of the subcarrier.

Load modulation with a subcarrier creates two modulation sidebands at the reader's antenna at the distance of the subcarrier frequency around the operating frequency f_{READER}. These modulation sidebands can be separated from the significantly stronger signal of the reader by bandpass (BP) filtering on one of the two frequencies $f_{READER} \pm f_s$. Once it has been amplified, the subcarrier signal is now very simple to demodulate.

Because of the large bandwidth required for the transmission of a subcarrier, this procedure can only be used in the ISM frequency ranges for which this is permitted, 6.78 MHz, 13.56 MHz and 27.125 MHz.

➢ *Subharmonic procedure*

The subharmonic of a sinusoidal voltage A with a defined frequency f_A is a sinusoidal voltage B, whose frequency f_B is derived from an integer division of the frequency f_A. The subharmonics of the frequency f_A are therefore the frequencies $f_A/2$, $f_A/3$, $f_A/4$, ...

In the subharmonic transfer procedure, a second frequency f_B , which is usually lower by a factor of two, is derived by digital division by two of the reader's transmission frequency f_A. The output signal f_B of a binary divider can now be modulated with the data stream from the transponder. The modulated signal is then fed back into the transponder's antenna via an output driver.

One popular operating frequency for subharmonic systems is 128kHz. This gives rise to a transponder response frequency of 64 kHz.

2.3.1.2 Electromagnetic Backscatter Coupling

RFID systems in which the gap between the reader and transponder is greater than 1 m are called *long-range systems*. These systems are operated at the UHF frequencies of 868 MHz (Europe) and 915 MHz (USA), and at the microwave frequencies 2.5 GHz and 5.8 GHz. The short wavelengths of these frequency ranges facilitate the construction of antennas with far smaller dimensions and greater efficiency than would be possible using frequency ranges below 30 MHz.

In order to achieve long ranges of up to 15 m or to be able to operate transponder chips with greater power consumption at an acceptable range, backscatter transponders often have a backup battery to supply power to the transponder chip. To prevent this battery from being loaded unnecessarily, the microchips generally have a power saving 'power down' or 'stand-by' mode. If the transponder moves out of range of a reader, then the chip automatically switches over to the power saving 'power down' mode. In this state the power consumption is a few μA at most. The chip is not reactivated until a sufficiently strong signal is received in the read range of a reader, whereupon it switches back to normal operation. However, the battery of an active transponder never provides power for the transmission of data between transponder and reader, but serves exclusively for the supply of the microchip. Data transmission between transponder and reader relies exclusively upon the power of the electromagnetic field emitted by the reader.

Power supply to the transponder

We know from the field of *RADAR technology* that electromagnetic waves are reflected by objects with dimensions greater than around half the wavelength of the wave. The efficiency with which an object reflects electromagnetic waves is described by its *reflection cross-section.* Objects that are in resonance with the wave front that hits them, as is the case for antenna at the appropriate frequency for example, have a particularly large reflection cross-section.

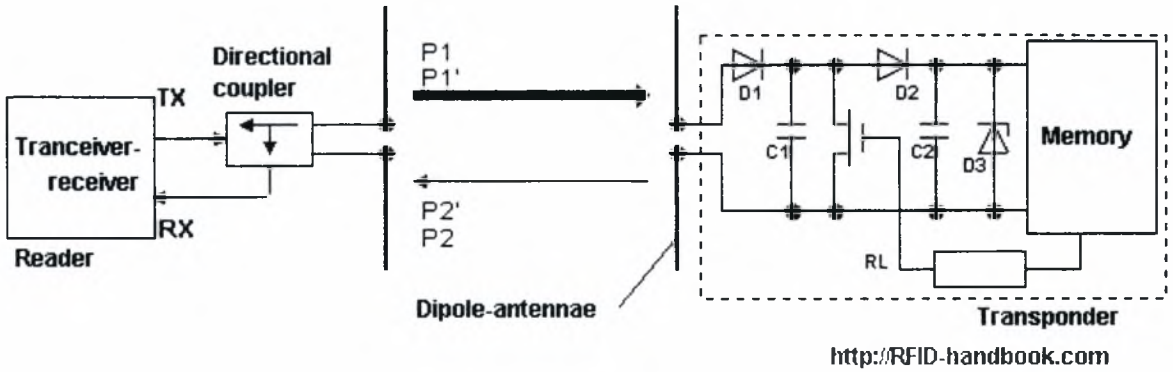

Figure 2.8: Operating principle of a backscatter transponder.

Power P1 is emitted from the reader's antenna, a small proportion of which (due to free space attenuation) reaches the transponder's antenna (***figure 2.8***). The power P1' is supplied to the antenna connections as HF voltage and after rectification by the diodes D1 and D2 this can be used as turn-on voltage for the deactivation or activation of the power saving "power-down" mode. The diodes used here are *low barrier Schottky diodes*, which have a particularly low threshold voltage. The voltage obtained may also be sufficient to serve as a power supply for short ranges.

Data transfer from transponder to reader

A proportion of the incoming power P1' is reflected by the antenna and returned as power P2. The reflection characteristics (= reflection cross-section) of the antenna can be influenced by altering the load connected to the antenna. In order to transmit data from the transponder to the reader, a load resistor RL connected in parallel with the antenna is switched on and off in time with the data stream to be transmitted. The amplitude of the power P2 reflected from the transponder can thus be modulated (→ modulated backscatter).

The power P2 reflected from the transponder is radiated into free space. A small proportion of this (free space attenuation) is picked up by the reader's antenna. The reflected signal therefore travels into the antenna connection of the reader in the "backwards direction" and can be decoupled using a *directional coupler* and transferred to the receiver input of a reader. The "forward" signal of the transmitter, which is stronger by powers of ten, is to a large degree suppressed by the directional coupler.

The ratio of power transmitted by the reader and power returning from the transponder (P1 / P2) can be estimated using the radar equation.

Power supply to the transponder

Close coupling systems are designed for ranges between 0.1 cm and a maximum of 1 cm. The transponder is therefore inserted into the reader or placed onto a marked surface ('touch & go') for operation.

Inserting the transponder into the reader, or placing it on the reader, allows the transponder coil to be precisely positioned in the *air gap* of a ring-shaped or U – shaped core. The functional layout of the transponder coil and reader coil corresponds with that of a transformer (***figure 2.9***). The reader represents the primary winding and the transponder coil represents the secondary winding of the transformer. A high frequency alternating current in the primary winding generates a high frequency magnetic field in the core and air gap of the arrangement, which also flows through the transponder coil. This power is rectified to provide a power supply to the chip.

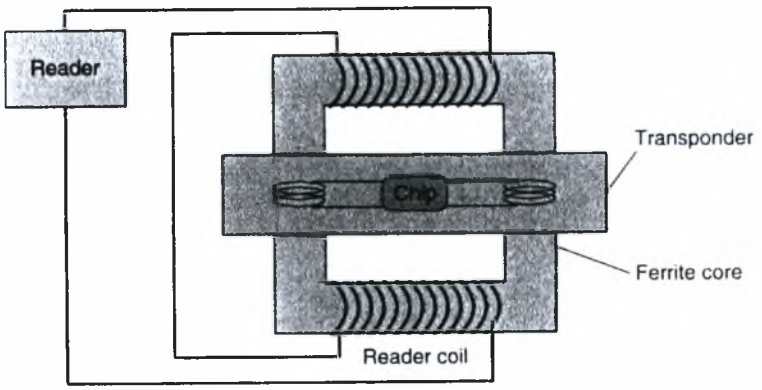

Figure 2.9: Close coupling transponder in an insertion reader with magnetic coupling coils.

Because the voltage U induced in the transponder coil is proportional to the frequency f of the exciting current, the frequency selected for power transfer should be as high as possible. In practice, frequencies in the range 1 – 10 MHz are used. In order to keep the losses in the transformer core low, a ferrite material that is suitable for this frequency must be selected as the core material.

Because, in contrast to inductively coupled or microwave systems, the efficiency or power transfer from reader to transponder is very good, close coupling systems are excellently suited for the operation of chips with high power consumption. This includes microprocessors, which still require some 10 mW power for operation. For this reason, the close coupling chip card systems on the market all contain microprocessors.

The mechanical and electrical parameters of contactless close coupling chip cards are defined in their own standard, ISO 10536. For other designs the operating parameters can be freely defined.

Data transfer from transponder to reader

➢ *Magnetic coupling*

Load modulation with subcarrier is also used for magnetically coupled data transfer from the transponder to the reader in close coupling systems. Subcarrier frequency and modulation is specified in ISO 10536 for close coupling chip cards.

➢ *Capacitive coupling*

Due to the short distance between the reader and transponder, close coupling systems may also employ *capacitive coupling* for data transmission. Plate capacitors are constructed from coupling surfaces isolated from one another, and these are arranged in the transponder and reader in such way that when a transponder is inserted they are exactly parallel to one another.

This procedure is also used in close coupling smart cards. The mechanical and electrical characteristics of these cards are defined in ISO 10536.

2.3.1.4 Electrical Coupling

Power supply to passive transponders

In *electrically (i.e. capacitively)* coupled systems the reader generates a strong, high-frequency *electrical field.* The reader's antenna consists of a large, electrically conductive area (*electrode*), generally a metal foil or a metal plate. If a high-frequency voltage is applied to the electrode a high-frequency electric field forms between the electrode and the earth potential (ground). The voltages required for this, ranging between a few hundreds volts and a few thousand volts, are generated by voltage rise in a resonant circuit made up of a coil L_1 in the reader, plus the parallel connection of an internal capacitor C_1 and the capacitance active between the electrode and the earth potential $C_{R\text{-}GND}$. The resonant frequency of the resonant circuit corresponds with the transmission frequency of the reader.

The antenna of the transponder is made up of two conductive surfaces lying in a plane (electrodes). If the transponder is placed within the electrical field of the reader, then an electric voltage arises between the two transponder electrodes, which is used to supply power to the transponder chip (***figure 2.10***).

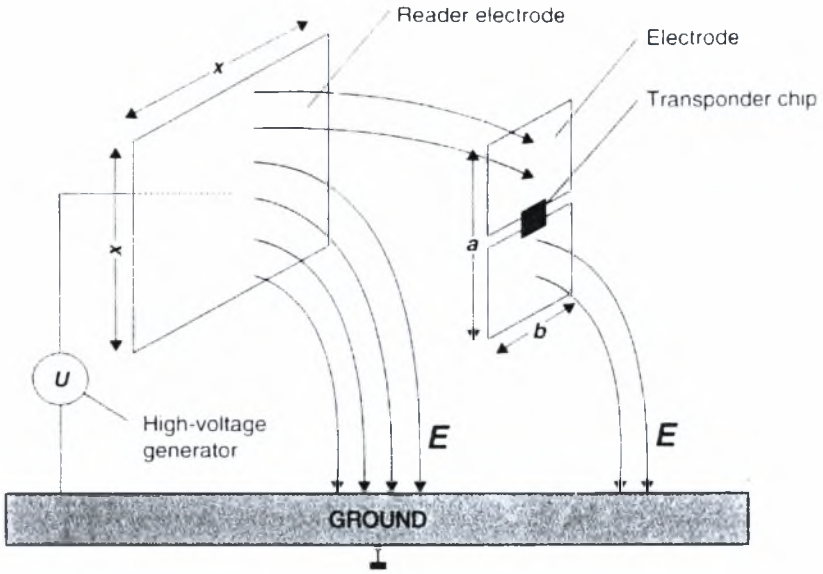

Figure 2.10: An electrically coupled system uses electrical (electrostatic) fields for the transmission of energy and data.

Since a capacitor is active both between the transponder and the transmission antenna ($C_{R\text{-}T}$) and between the transponder antenna and the earth potential ($C_{T\text{-}GND}$) the equivalent circuit diagram for an electrical coupled RFID system can be considered in a simplified form as a *voltage divider* with the elements $C_{R\text{-}T}$, R_L (input resistance of the transponder) and $C_{T\text{-}GND}$ (***figure 2.11***).

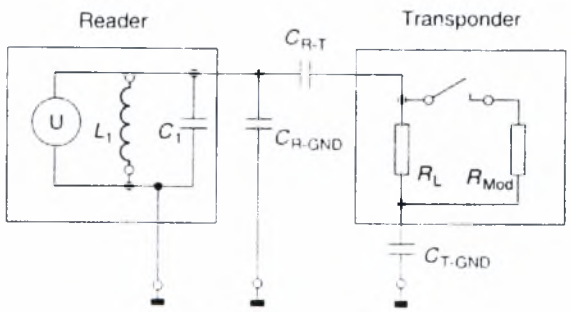

Figure 2.11: Equivalent circuit diagram of an electrically coupled RFID system.

The currents that flow in the electrode surfaces of the transponder are very small. Therefore, no particular requirements are imposed upon the conductivity of the electrode material. In addition to the normal metal surfaces (metal foil) the electrodes can thus also be made of conductive colours (e.g. a *silver conductive paste*) or a *graphite coating*.

Data transfer from transponder to reader

If an electrically coupled transponder is placed within the interrogation zone of a reader, the input resistance R_L of the transponder acts upon the resonant circuit of the reader via the coupling capacitance C_{R-T} active between the reader and transponder electrodes, damping the resonant circuit slightly. This damping can be switched between two values by switching a modulation resistor R_{mod} in the transponder on and off. Switching the modulation resistor R_{mod} on and off thereby generates an amplitude modulation of the voltage present at L_1 and C_1 by the remote transponder. By switching the modulation resistor R_{mod} on and off in time with data, this data can be transmitted to the reader. This procedure is called *load modulation*.

2.3.1.5 Data transfer from reader to transponder

All known digital modulation procedures are used in data transfer from the reader to the transponder in full and half duplex systems, irrespective of the operating frequency of the coupling procedure. There are three basic procedures:

- **ASK**: amplitude shift keying
- **FSK**: frequency shift keying
- **PSK**: phase shift keying

Because of the simplicity of demodulation, the majority of systems use ASK modulation.

2.3.2 Sequential Procedures

2.3.2.1 Inductive Coupling

Power supply to the transponder

Sequential systems using inductive coupling are operated exclusively at frequencies below 135 kHz. A transformer type coupling is created between the reader's coil and the transponder's coil. The induced voltage generated in the transponder coil by the effect of an alternating field from the reader is rectified and can be used as a power supply.

In order to achieve higher efficiency of data transfer, the transponder frequency must be precisely matched to that of the reader, and the quality of the transponder coil must be carefully specified. For this reason the transponder contains an *on-chip trimming capacitor* to compensate for resonant frequency manufacturing tolerances.

However, unlike full and half duplex systems, in sequential systems the reader's transmitter does not operate on a continuous basis. The energy transferred to the transmitter during the transmission operation charges up a *charging capacitor* to provide an energy store. The transponder chip is switched over to stand-by or power saving mode during the charging operation, so that almost all of the energy received is used to charge

up the charging capacitor. After a fixed charging period the reader's transmitter is switched off again.

The energy stored in the transponder is used to send a reply to the reader. The minimum capacitance of the charging capacitor can be calculated from the necessary operating voltage and the chip's power consumption:

$$C = Q / U = I\,t / [V_{max} - V_{min}]$$

where Vmax, Vmin are limit values for operating voltage that may not be exceeded, I is the power consumption of the chip during operation and t is the time required for the transmission of data fro transponder to reader.

Data transfer from transponder to reader

In sequential systems (***figure 2.12***) a full read cycle consists of two phases, the charging phase and the reading phase. The end of the charging phase is detected by an *end of burst detector*, which monitors the path of voltage at the transponder coil and thus recognises the moment when the reader's field is switched off. At the end of the charging phase an on-chip oscillator, which uses the resonant circuit formed by the transponder coil as a frequency determining component, is activated. A weak magnetic alternating field is generated by the transponder coil, and this can be received by the reader. This gives an improved signal-interference distance of typically 20 dB compared to full/half duplex systems, which has a positive effect upon the ranges that can be achieved using sequential systems.

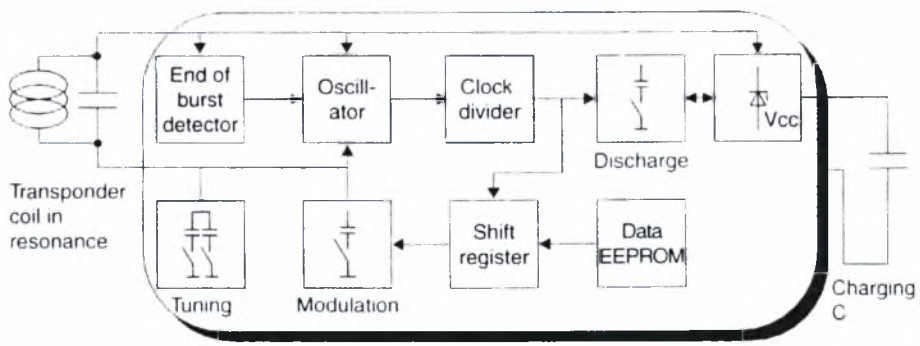

Figure 2.12: Block diagram of a sequential transponder using inductive coupling.

The transmission frequency of the transponder corresponds with the resonant frequency of the transponder coil, which was adjusted to the transmission frequency of the reader when it was generated.

In order to be able to modulate the HF signal generated in the absence of a power supply, an additional modulation capacitor is connected in parallel with the resonant circuit in time with the data flow. The resulting frequency shift keying provides a 2 *FSK modulation.*

After all the data has been transmitted, the discharge mode is activated to fully discharge the charging capacitor. This guarantees a safe Power-On-Reset at the start of the next charging cycle.

2.3.2.1 Surface acoustic wave transponder

Surface acoustic wave transponder (SAW) devices are based upon the piezoelectric effect and on the surface-related dispersion of elastic (=acoustic) waves at low speed. If an (ionic) crystal is elastically deformed in a certain direction, surface charges occur, giving rise to electric voltages in the crystal (application: piezo lighter). Conversely, the application of a surface charge to a crystal leads to an elastic deformation in the crystal grid (application: piezo buzzer). Surface acoustic wave devices are operated at microwave frequencies, normally in the ISM range2.45 GHz.

Electroacoustic transducers (interdigital transducers) and reflectors can be created using planar electrode structures on piezoelectric substrates. The normal substrate used for this application is lithium niobate or lithium tantalite. The electrode structure is created by a photolithographic procedure, similar to the procedure used in microelectronics for the manufacture of integrated circuits.

Figure 2.13 illustrates the basic layout of a surface wave transponder. A finger-shaped electrode structure – the *interdigital transducer* – is positioned at the end of a long piezoelectrical substrate, and a suitable *dipole antenna* for the operating frequency is attached to its busbar. The interdigital transducer is used to convert between electrical signals and acoustic surface waves.

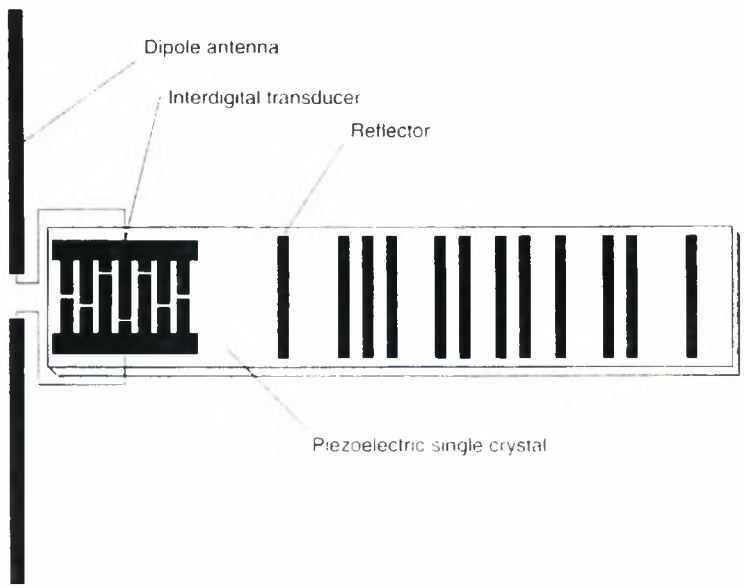

Figure 2.13: Basic layout of an SAW transponder. Interdigital transducers and reflectors are positioned on the piezoelectric crystal.

An electrical impulse applied to the busbar causes a mechanical deformation to the surface of the substrate due to the piezoelectrical effect between the electrodes (fingers), which disperses in both directions in the form of a surface wave (rayleigh wave). For a normal substrate the dispersion speed lies between 3000 and 4000 m/s. Similarly, a surface wave entering the converter creates an electrical impulse at the busbar of the interdigital transducer due to the piezoelectric effect.

Individual electrodes are positioned along the remaining length of the surface wave transponder. The edges of the electrodes form a reflective strip and reflect a small proportion of the incoming surface waves. Reflector strips are normally made of aluminium; however some reflector strips are also in the form of etched grooves.

A high frequency *scanning pulse* generated by a reader is supplied from the dipole antenna of the transponder into the interdigital transducer and is thus converted into an acoustic surface wave, which flows through the substrate in the longitudinal direction. The frequency of the surface wave corresponds with the carrier frequency of the sampling pulse (e.g. 2.45 GHz). The carrier frequency of the reflected and returned pulse sequence thus corresponds with the transmission frequency of the sampling pulse.

Part of the surface wave is reflected off each of the reflective strips that are distributed across the substrate, while remaining part of the surface wave continues to travel to the end of the substrate and is absorbed there.

The reflected parts of the wave travel back to the interdigital transducer, where they are converted into a high frequency pulse sequence and are emitted by the dipole antenna. This pulse sequence can be received by the reader. The number of pulses received corresponds with the number of reflective strips on the substrate. Likewise, the delay between the individual pulses is proportional to the spatial distance between the reflector strips on the substrate, and so the spatial layout of the reflector strips can represent a binary sequence of digits.

Due to the slow dispersion speed of the surface waves on the substrate the first response pulse is only received by the reader after a dead time of around 1.5 ms after the transmission of the scanning pulse. This gives decisive advantages for the reception of the pulse.

The range of a surface wave system depends mainly upon the transmission power of the scanning pulse and can be estimated using the radar equation. At the permissible transmission power in the 2.45 GHz ISM frequency range, a range of 1-2 m can be expected.

2.3 Frequency, Range and Coupling

The most important differentiation criteria for RFID systems are the operating frequency of the reader, the physical coupling method and the range of the system. RFID systems are operated at widely differing frequencies ranging from 135 kHz longwave to 5.8 GHz in the microwave range. *Electric*, *magnetic* and *electromagnetic fields* are used for the physical coupling. Finally, the achievable range of the system varies from a few millimetres to above 15 m.

RFID systems with a very small range, typically in the region of up to 1 cm, are known as *close coupling systems*. For operation the transponder must either be inserted into the reader or positioned upon a surface provided for this purpose. Close coupling systems are coupled using both electric and magnetic fields and can theoretically be operated at any desired frequency between DC and 30 MHz because the operation of the transponder does not rely upon the radiation of fields. The close coupling between the data carrier and reader also facilitated the provision of greater amounts of power and so even a microprocessor with non-optimal power consumption, for example, can be operated. Close coupling systems are primarily used in applications that are subject to strict security requirements, but do not require a large range. Examples are electronic door locking systems or contactless smart card systems with payment functions. Close coupling transponders are currently used exclusively as ID-1 format contactless smart cards (ISO 10536). However, the role of close coupling systems on the market is becoming less important.

Systems with write and read ranges of up to 1 m are known by the collective term of remote coupling systems. Almost all *remote coupled systems* are based upon an *inductive (magnetic) coupling* between reader and transponder. These systems are therefore also known as *inductive radio systems*. In addition there are also a few systems with *capacitive (electric) coupling*. At least 90% of all RFID systems currently sold are inductively coupled systems. For this reason there is now an enormous number of such systems on the market. Frequencies below 135 kHz or 13.56 MHz are used as transmission frequencies. Some special applications are also operated at 27.125 MHz.

RFID systems with ranges significantly above 1 m are known as *long-range systems*. All long-range systems operate using electromagnetic waves in the *UHF* and *microwave range*. The vast majority of such systems are also known as *backscatter systems* due to their physical operating principle. In addition, there are also long-range systems using *surface acoustic wave transponders* in the microwave range. All these systems are operated at the UHF frequencies of 868 MHz (Europe) and 915 MHz (USA) and at the microwave frequencies of 2.5 GHz and 5.8 GHz. Typical ranges of 3m can now be achieved using passive (battery-free) backscatter transponders, while ranges of 15 m and above can even be achieved using active (battery-supported) backscatter transponders. The battery of an active transponder, however, never provides the power for data transmission between transponder and reader, but serves exclusively to supply the microchip and for the retention of stored data. The power of electromagnetic field

received from the reader is the only power used for the data transmission between the transponder and reader.

3. Readers

The reader's main functions are to activate the data carrier (transponder), structure the communication sequence with the data carrier and transfer data between the application software and a contactless data carrier. All features of the contactless communication, i.e. making the connection and performing anticollision and authentication procedures are handled entirely by the reader.

Despite the fundamental differences in the type of coupling (inductive-electromagnetic), the communication sequence (FDX, HDX, SEQ), the data transmission procedure from the transponder to the reader (load modulation, backscatter, subharmonic) and, last but not least, the frequency range, all readers are similar in their basic operating principle and thus in their design. Readers in all systems can be reduced to two fundamental functional blocks: the ***control system*** and the ***HF interface***, consisting of a transmitter and receiver (***figure 3.1***).

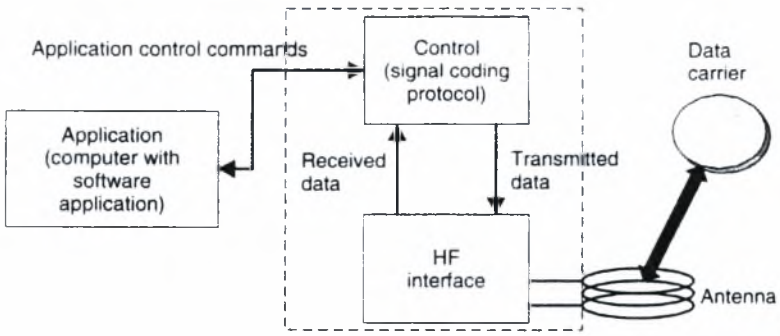

Figure 3.1: Block diagram of a reader consisting of a control system and HF interface. The entire system is controlled by an external application via control commands.

3.1 HF Interface

The reader's HF interface performs the following functions:

- generation of high frequency transmission power to activate the transponder and supply it with power;
- modulation of the transmission signal to send data to the transponder;
- reception and demodulation of HF signals transmitted by a transponder.

The HF interface contains two separate signal paths to correspond with the two directions of data flow from and to the transponder (***figure 3.2***). Data transmitted to the transponder travels through the *transmitter arm*. Conversely, data received from the transponder is processed in the *receiver arm*.

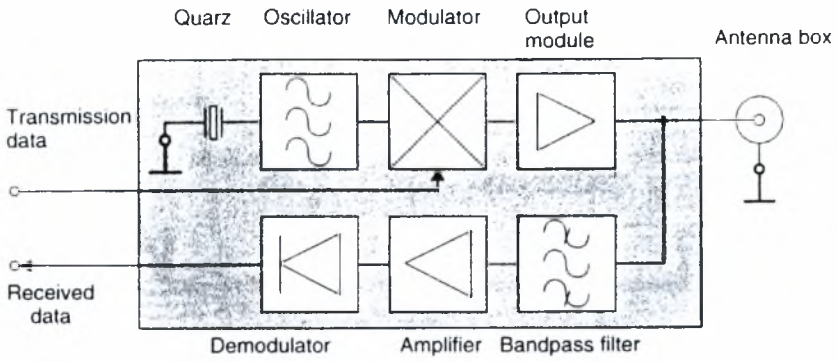

Figure 3.2: Block diagram of an HF interface for an inductively coupled RFID system.

In the following sections, the two signal channels will be analysed in more detail, giving consideration to the differences between the different systems.

3.1.1 Inductively coupled system, FDX/HDX

Transmitter arm

First, a signal of the required operating frequency, i.e. 135 kHz or 13.56 MHz, is generated in the transmitter arm by a stable (frequency) quartz oscillator. To avoid worsening the noise ratio in relation to the extremely weak received signal from the transponder, the oscillator is subject to high demands regarding phase stability and sideband noise.

The oscillator signal is fed into a modulation module controlled by the baseband signal of the signal coding system. This baseband signal is a keyed direct voltage signal (TTL level), in which the binary data is represented using a serial code (Manchester, Miller, NRZ). Depending upon the modulator type, ASK or PSK modulation is performed on the oscillator signal. FSK modulation is also possible, in which case the baseband signal is fed directly into the frequency synthesiser.

The modulated signal is then brought to the required level by a power output module and can then be decoupled to the antenna box.

Receiver arm

The receiver arm begins at the antenna box, with the first component being a steep edge bandpass filter or a notch filter. In FDX/HDX systems this filter has the task of largely blocking the strong signal from the transmission output module and filtering out just the response signal from the transponder.

In subharmonic systems, this is a simple process, because transmission and reception frequencies are usually a whole octave apart. In systems with load modulation using a

subcarrier the task of developing a suitable filter should not be underestimated because, in this case, the transmitted and received signals are only separated by the carrier frequency. Typical subcarrier frequencies in 13.56 MHz systems are 847kHz or 212 kHz.

Some LF systems with load modulation and no subcarrier use a notch filter to increase the modulation depth (duty factor) - the ratio of the level to the load modulation sidebands - and thus the duty factor by reducing their own carrier signal. A different procedure is the rectification and thus demodulation of the (load) amplitude modulated voltage directly at the reader antenna.

3.1.2 Microwave systems – HDX

The main difference between microwave systems and low frequency inductive systems is the frequency synthesising: the operating frequency, typically 2.45 GHz, cannot be generated directly by the quartz oscillator, but is created by the multiplication (excitation of harmonics) of a lower oscillator frequency. Because the modulation is retained during frequency multiplication, modulation is performed at the lower frequency (***figure 3.3***).

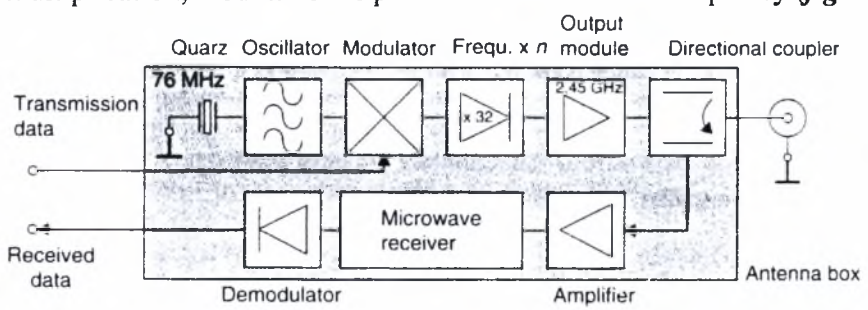

Figure 3.3: Block diagram of an HF interface for microwave systems.

Some microwave systems employ a directional coupler to separate the system's own transmission signal from the weak backscatter signal of the transponder. A directional coupler (***figure 3.4***) consists of two continuously coupled homogeneous wires. If all four ports are matched and power P_1 is supplied to port 1, then the power is divided between ports 2 and 3, with no power occurring at the decoupled port 4. The same applies if power is supplied to port 3, in which case the power is divided between ports 1 and 2.

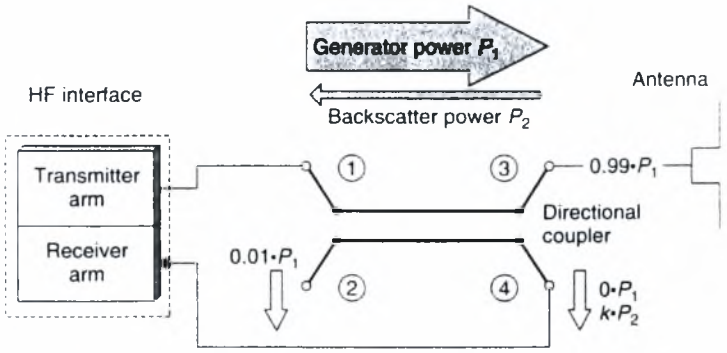

Figure 3.4: Layout and operating principle of a directional coupler for a backscatter RFID system.

3.1.3 Sequential systems – SEQ

In a sequential RFID system the HF field of the reader is only ever transmitted briefly to supply the transponder with power and/or send commands to the transponder. The transponder transmits its data to the reader while the reader is not transmitting. The transmitter and receiver in the reader are thus active sequentially, like a walkie-talkie, which also transmits and receives alternately.

The reader (***figure 3.5***) contains an instantaneous switching unit to switch between transmitter and receiver mode. This function is normally performed by PIN diodes in radio technology.

No special demands are made of the receiver in an SEQ system. Because the strong signal of the transmitter is not present to cause interference during reception, the SEQ receiver can be designed to maximize sensitivity. This means that the range of the system as a whole can be increased to correspond with the energy range, i.e. the distance between the reader and transponder to which there is just enough energy for the operation of the transponder.

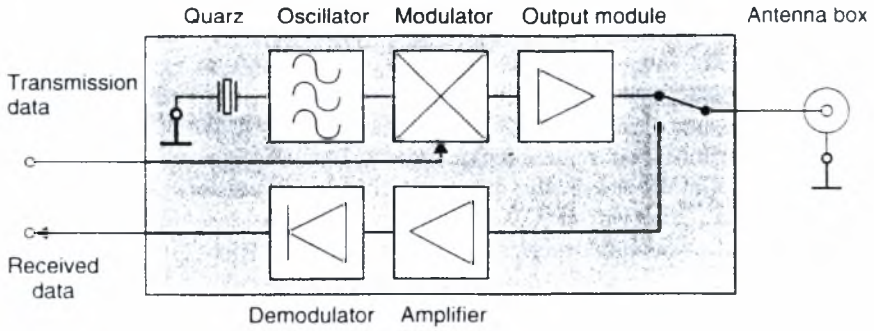

Figure 3.5: HF interface for a sequential reader system.

3.1.4 Microwave system for SAW transponders

A short electromagnetic pulse transmitted by the reader's antenna is received by the antenna of the *surface wave transponder* and converted into a surface wave in a piezoelectric crystal. A characteristic arrangement of partially reflective structures in the propagation path of the surface wave gives rise to numerous pulses, which are transmitted back from the transponder's antenna as a response signal.

Due to the propagation delay times in the piezoelectric crystal the coded signal reflected by the transponder can easily be separated in the reader from all other electromagnetic reflections from the vicinity of the reader. The block diagram of a reader for surface wave transponders is shown in ***figure 3.6***.

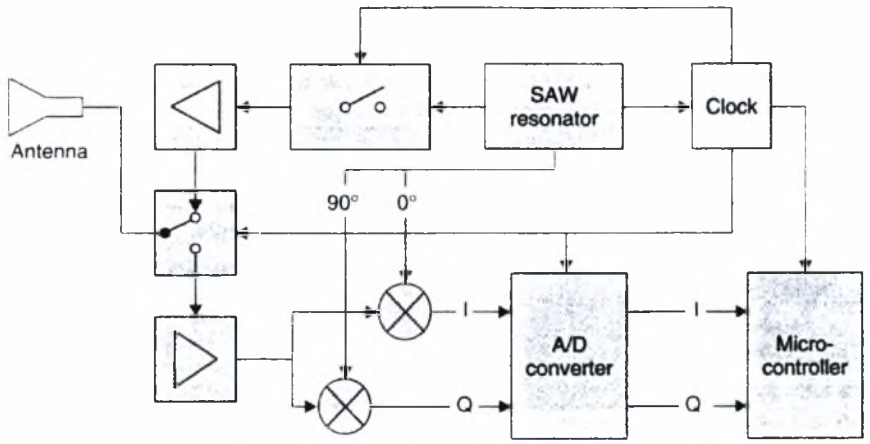

Figure 3.6: Block diagram of a reader for a surface wave transponder.

A stable frequency and phase oscillator with a surface wave resonator is used as the high-frequency source. Using a rapid HF switch, short HF pulses of around 80 ns duration are generated from the oscillator signal, which are amplified to around 36 dBm (4 W peak) by the connected power output stage, and transmitted by the reader's antenna.

If a SAW transponder is located in the vicinity of the reader it reflects a sequence of individual pulses after a propagation delay time of a few microseconds. The pulses received by the reader's antenna pass through a low-noise amplifier and are then demodulated in a quadrature demodulator. This yields two orthogonal components (I and Q), which facilitate the determination of the phase angle between the individual pulses and between the pulses and the oscillator. The information obtained can be used to determine the distance or speed between SAW transponder and reader and for the measurement of physical quantities.

3.2 Control Unit

The reader's control unit (***figure 3.7***) performs the following functions:

- communication with the application software and execution of commands from the application software;
- control of the communication with a transponder (master-slave principle);
- signal coding and decoding

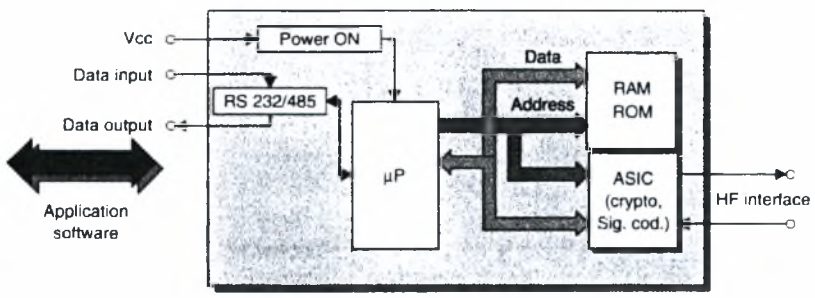

Figure 3.7: Block diagram of the control unit of a reader. There is a serial interface for communication with the higher application software.

In more complex systems the following additional functions are available:

- execution of an anticollision algorithm;
- encryption and decryption of the data to be transferred between transponder and reader;
- performance of authentication between transponder and reader.

The control unit is usually based upon a microprocessor to perform these complex functions. Cryptological procedures, such as stream ciphering between transponder and reader, and also signal coding, are often performed in an additional ASIC module to relieve the processor of calculating intensive processes. For performance reasons the ASIC is accessed via the microprocessor bus (register orientated).

Data exchange between the application software and the reader's control unit is performed by an RS232 or RS485 interface. As is normal in the PC world, NRZ coding (8-bit asynchronous) us used. The baud rate is normally a multiple of 1200Bd(4800 Bd, 9600 Bd, etc.). Various, often self-defined, protocols are used as the communication protocol.

The interface between the HF interface and the control unit represents the state of the HF interface as a binary number. In an ASK modulated system a logic '1' at the modulation input of the HF interface represents the state 'HF signal on'; a logic'0' represents the state 'HF signal off'.

4. Transponders

The data carriers in RFID systems are divided into electronic data carriers based upon integrated circuits (microchips) and data carriers that exploit physical effects for data storage. Electronic data carriers are further subdivided into data carriers with a pure memory function and those that incorporate a programmable microprocessor. Both 1-bit transponders and surface acoustic wave (SAW) transponders are data carriers that exploit physical effects for data storage.

This chapter deals exclusively with the functionality of electronic data carriers. The simple functionality of physical data carriers has already been described in Chapter 2.

4.1 Transponder with Memory Function

Transponders with a memory function (***figure 4.1***) contain RAM, ROM, EEPROM or FRAM and an HF interface to provide the power supply and permit communication with the reader. The main distinguishing characteristic of this family of transponders is the realization of address and security logic on the chip using a state machine.

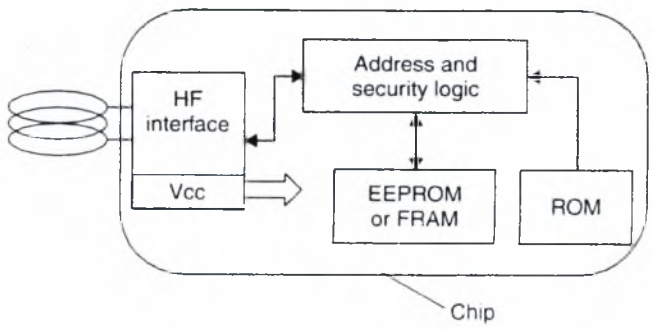

Figure 4.1: Block diagram of an RFID data carrier with a memory function.

4.1.1 HF interface

The HF interface forms the interface between the analogue, high frequency transmission channel from the reader to the transponder and the digital circuitry of the transponder. The HF interface therefore performs the functions of a classical modem (modulator-demodulator) used for analogue data trasmission via telephone lines.

The modulated HF signal from the reader is reconstructed in the HF interface by demodulation to create a digital serial data stream for reprocessing in the address and

security logic. A clock-pulse generation circuit generates the system clock for the data carrier from the carrier frequency of the HF field.

The HF interface incorporates a load modulator or backscatter modulator (or an alternative procedure, e.g. frequency divider), controlled by the digital data being transmitted, to return data to the reader (***figure 4.2***)

Passive transponders, i.e. transponders that do not have their own power supply, are supplied with energy via the HF field of the reader. To achieve this, the HF interface draws current from the transponder antenna, which is rectified and supplied to the chip as a regulated supply voltage.

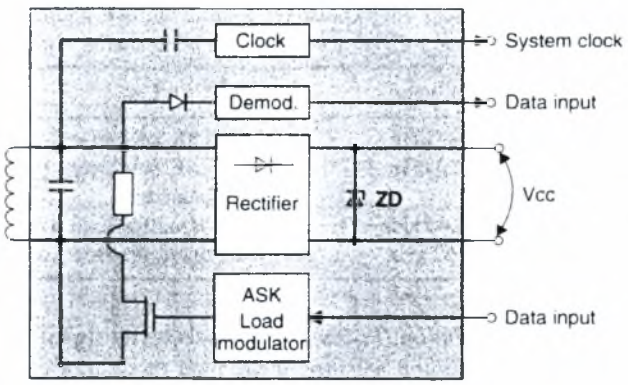

Figure 4.2: Block diagram of the HF interface of an inductively coupled transponder with a load modulator.

4.1.1.1 Example circuit – load modulation with subcarrier

The principal base circuit of a load modulator is shown in ***figure 4.3***. This generates an ohmic load modulation using an ASK or FSK modulated subcarrier. The frequency of the subcarrier and the baud rates are in accordance with the specifications of the standard ISO 15693 (vicinity coupling smart cards).

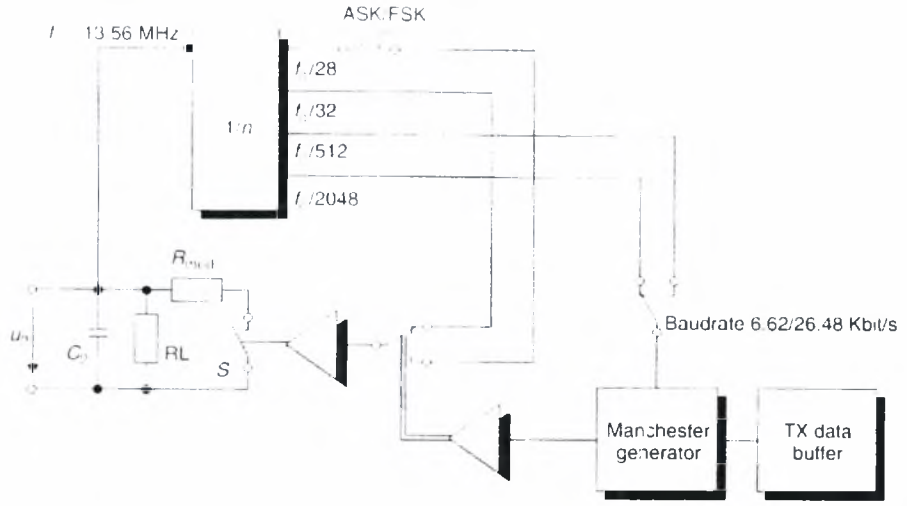

Figure 4.3: Generation of a load modulation with modulated subcarrier: the subcarrier frequency is generated by a binary division of the carrier frequency of the RFID system. The subcarrier signal itself is initially ASK of FSK modulated (switch position ASK/FSK) by the Manchester coded data stram, while the modulation resistor in the transponder is finally switched on and off in time with the modulated subcarrier signal.

The high-frequency input voltage u_2 of the data carrier (transponder chip) serves as the time basis of the HF interface and is passed to the input of a binary divider. The frequencies specified in the standard for the subcarrier and the baud rate can be derived from the single binary division of the 13.56 MHz input signal (***figure 4.4***).

Splitter N	Frequency	Use
1/28	485 kHz	φ2 of the FSK subcarrier
1/32	423 kHz	φ1 of the FSK subcarrier, plus ASK subcarrier
1/512	26.48 kHz	Bit clock signal for high baud rate
1/2048	6.62 kHz	Bit clock signal for slow baud rate

Figure 4.4: The clock frequencies required in the HF interface are generated by the binary division of the 13.56 MHz carrier signal.

The serial data to be transmitted is first transferred to a Manchester generator. This allows the baud rate of the baseband signal to be adjusted between two values. The Manchester coded baseband signal is now used to switch between the two subcarrier frequencies f_1 and f_2 using the '1' and '0' levels of the signal, in order to generate an FSK modulated subcarrier signal. If the clock signal f_2 is interrupts, this results in an ASK modulated subcarrier signal, which means that it is very simple to switch between ASK and FSK modulation. The modulated subcarrier signal is now transferred to switch S, so

that the modulation resistor of the load modulator can be switched on and off in time with the subcarrier frequency.

4.1.2 Address and security logic

The *address and security logic* forms the heart of the data carrier and controls all processes on the chip (***figure 4.5***).

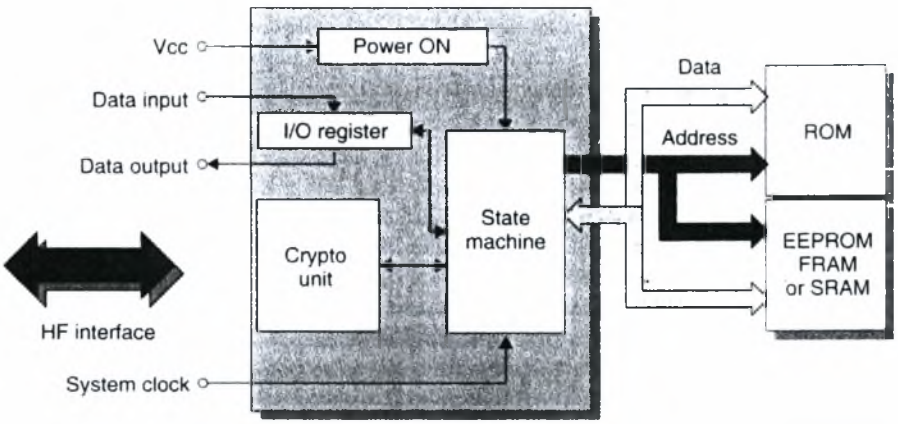

Figure 4.5: Block diagram of address and security logic module.

The *power on logic* ensures that the data carrier takes on a defined state as soon as it receives an adequate power supply upon entering the HF field of a reader. Special I/O registers perform the data exchange with the reader. An optional *cryptological unit* is required for authentication, data encryption and key administration.

The data memory, which comprises a ROM for permanent data such as serial numbers, and EEPROM or FRAM is connected to the address and security logic via the address and data bus inside the chip.

The *system clock* required for sequence control and system synchronisation is derived from the HF field by the HF interface and supplied to the address and security logic module. The state-dependent control of all procedures is performed by a state machine ('hard-wired software'). The complexity that can be achieved using state machines comfortably equals the performance of microprocessors. However, the 'programme sequence' of these machines is determined by the chip design. The functionality can only be changed or modified by modifying the chip design and this type of arrangement is thus only of interest for very large production runs.

4.1.2.1 State machine

A *state machine* (also switching device, Mealy machine) is an arrangement used for executing logic operations, which also has the capability of storing variable states (***figure 4.6***). The output variable Y depends upon both the input variable X and what has gone before, which is represented by the switching state of flip-flops. The state machine therefore passes through different states, which can be clearly represented in a *state diagram*.

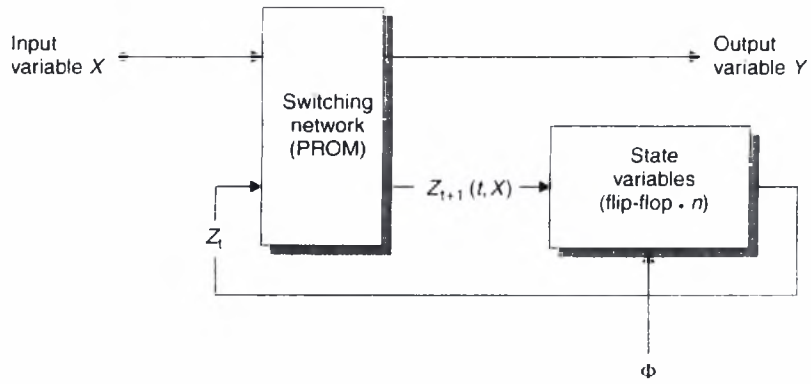

Figure 4.6: Block diagram of a state machine, consisting of the state memory and a backcoupled switching network.

4.1.3 Memory architecture

4.1.3.1 Read-only transponder

This type of transponder represents the low-end, low-cost segment of the range of RFID data carriers. As soon as a read-only transponder enters the interrogation zone of a reader it begins to continuously transmit its own identification number (***figure 4.7***). This identification number is normally a simple serial number of a few bytes with a check digit attached. Normally, the chip manufacturer guarantees that each serial number is only used once. More complex codes are also possible for special functions.

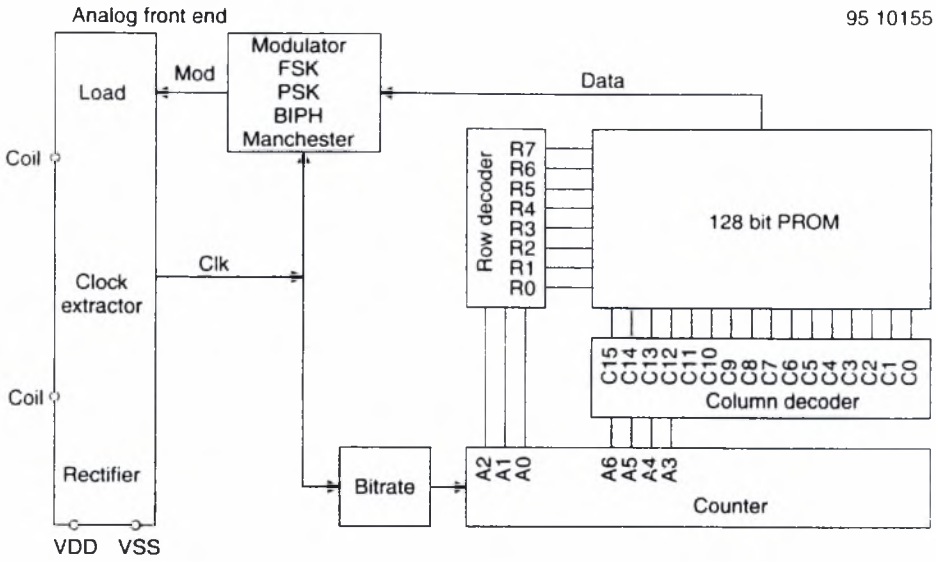

Figure 4.7: Block diagram of a read-only transponder. When the transponder enters the interrogation zone of a reader a counter begins to interrogate all addresses of the internal memory (PROM) sequentially. The data output of the memory is connected to a load modulator which is set to the baseband code of the binary code (modulator). In this manner the entire content of the memory (128-bit serial number) can be emitted cyclically as a serial data stream.

The transponder's unique identification number is incorporated into the transponders during chip manufacture. The user cannot alter this serial number or any data on the chip.

Communication with the reader is unidirectional, with the transponder sending its identification number to the reader continuously. Data transmission from the reader to the transponder is not possible. However, because of the simple layout of the data carrier and reader, read-only transponders can be manufactured extremely cheaply.

Read-only transponders are used in price-sensitive applications that do not require the option of storing data in the transponder. The classic fields of application are therefore animal identification, access control and industrial automation with central data management.

4.1.3.2 Writable transponder

Transponders that can be written with data by the reader are available with memory sizes ranging from just 1 byte ('pigeon transponder') to 64 Kbytes (microwave transponders with SRAM).

Write and read access to the transponder is often in blocks. When this is the case, a block is formed by assembling a predefined number of bytes, which can then be read or written as a single unit. To change the data content of an individual block, the entire block must

first be read from the transponder, after which the same block, including the modified bytes, can be written back to the transponder.

Current systems use block sizes of 16 bits, 4 bytes or 16 bytes. The block structure of the memory facilitates simple addressing in the chip and by the reader.

4.1.3.3 Transponder with cryptological function

If a writable transponder is not protected in some way, any reader that is part of the same RFID system can read from it, or write to it. This is not always desirable, because sensitive applications may be impaired by unauthorized reading or writing of data in the transponder. Two examples of such applications are the contactless cards used as tickets in the public transport system and the transponders in vehicle keys for electronic immobilization systems.

There are various procedures for preventing unauthorised access to a transponder. One of the simplest mechanisms is read and write protection by checking a password. In this procedure, the card compares the transmitted password with a stored reference password and permits access to the data memory if the passwords correspond.

However, if mutual authorization is to be sought or it is necessary to check that both components belong to the same application, then authentication procedures are used. Fundamentally, an authentication procedure always involves a comparison of two secret keys, which are not transmitted via the interface. Cryptological authentication is usually associated with the encryption of the data stream to be transmitted (***figure 4.8***). This provides an effective protection against attempts to eavesdrop into the data transmission by monitoring the wireless transponder interface using a radio receiver.

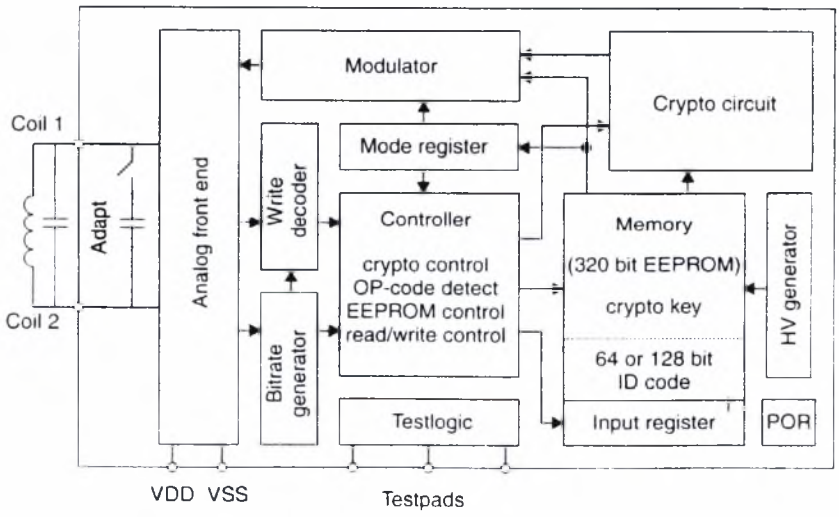

Figure 4.8: Block diagram of a writable transponder with a cryptological function to perform authentication between transponder and reader.

In addition to memory area allocated to application data, transponders with cryptological functions always have an additional memory area for the storage of the secret key and a configuration register (access register, Acc) for selectively write protecting selected address areas. The secret key is written to the key memory by the manufacturer before the transponder is supplied to the user. For security reasons, the key memory can never be read.

4.1.3.4 Segmented memory

Transponders can also be protected from access by readers that belong to other applications using authentication procedures. In transponders with large memory capacities, it is possible to divide the entire memory into small units called segments and protect each of these from unauthorized access with a separate key. A segmented transponder like this permits data from different applications to be stored completely separately.

Access to an individual segment can only be gained after successful authentication with the appropriate key. Therefore, a reader belonging to one application can only gain access to its 'own' segment if it only knows the application's own key.

The majority of segmented memory systems use fixed segment sizes. In these systems, the user cannot alter the storage space within a segment. A fixed segment size has the advantage that it is very simple and cheap to realize upon transponder's microchip.

However, it is very rare for the storage space required by an application to correspond with the segment size of the transponder. In small applications, valuable storage space on the transponder is wasted because the segments are only partially used. Very large applications, on the other hand, need to be distributed across several segments, which means that the application specific key must be stored in each of the occupied segments. This multiple storage of an identical key also wastes valuable storage space.

A much better use of space is achieved by the use of variable length segments. In this approach, the memory allocated to a segment can be matched to the requirements of the application using the memory area. Because of the difficulty in realizing variable segmentation, this variant is rare in transponders with state machines.

4.2 Transponder with Microprocessor

Transponders with microprocessors will become increasingly common in applications using contactless smart cards in the near future. Instead of the inflexible state machine, the transponder in these cards incorporates a microprocessor.

Industry standard microprocessors, such as the familiar 8051 or 6805, are used as the microprocessor at the heart of the chip. In addition, some manufacturers are offering

simple mathematical coprocessors (cryptological unit) on the same chip, which permit the rapid performance of the calculations required for encryption procedures. (***figure 4.9***).

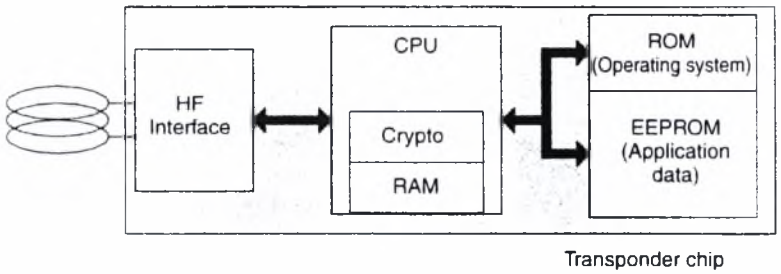

Figure 4.9: Block diagram of a writable transponder with a cryptological function to perform authentication between transponder and reader.

Contactless smart cards with microprocessors incorporate their own operating system, as has long been the case in contact-based cards. The tasks of the operating system in a contactless smart card are data transfer from an to the smart card, command sequence control, file management and the execution of cryptographic algorithms (e.g. encryption, authentication).

The programme modules are written in ROM code and are incorporated into the chip at the chip manufacturing stage by an additional exposure mask (mask programming).

The typical command processing sequence within a smart card operating system is as follows: commands sent from the reader to the contactless smart card are received by the smart card via the HF interface. Error recognition and correction mechanisms are performed by the I/O manager irrespective of higher-level procedures. An error-free command received by the secure messaging manager is decrypted or checked for integrity. After decryption the higher-level command interpreter attempts to decode the command. If this not possible, then the return code manager is called, which generates the appropriate return code and sends it back to the reader via the I/O manager (***figure 4.10***).

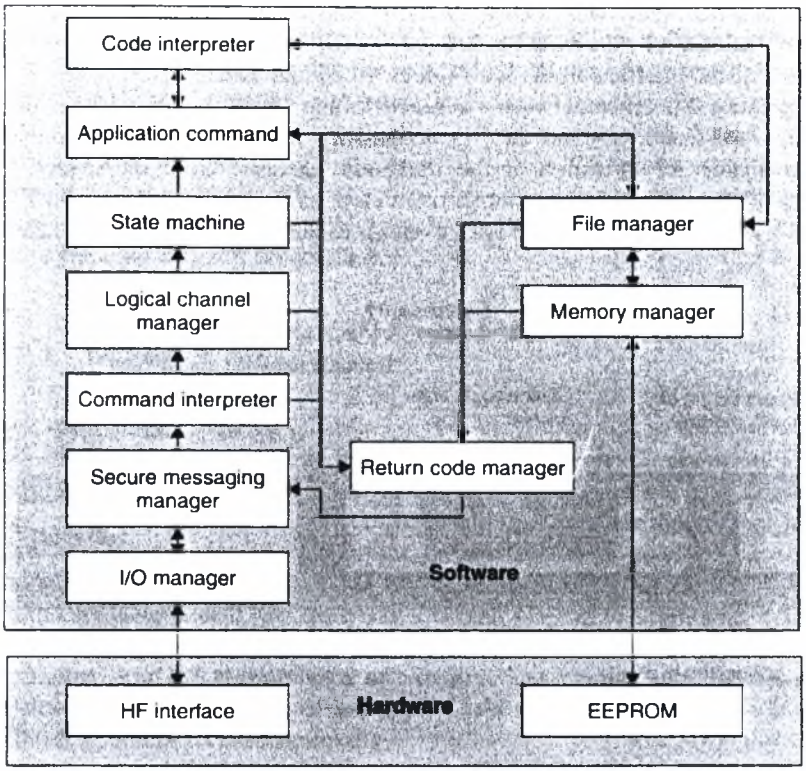

Figure 4.10: Command processing sequence within a smart card operating system.

If a valid command is received, then the actual programme code associated with this application command is executed. If access to the application data in the EEPROM is necessary, this is performed exclusively by the file management system and the memory manager, which convert all symbolic addresses into the corresponding physical addresses of the memory area. The file manager also checks access conditions (authorization) for the data in question.

4.3 Types of RFID Transponders

The types of RFID transponders, each type designed for a specific application, are the following:

- **Passive Transponders**

A transponder is said to be "passive" if it does not contain its own power source. The passive transponder picks up power from a nearby electric or magnetic field provided by a reader. The reader interrogates the adjacent field for transponders that may be in its proximity and induces enough energy into the transponder's electronic circuitry that it wakes up and transmits back to the reader its identification number as well as any additional data it may have stored in its memory.

The advantage of the passive transponder is that they are low cost, small and they virtually never require a battery change. The disadvantage is that they have relatively limited range. It is ideal for an identification label that will be scanned at close proximity. It is typically not a good solution for the detection of vehicles approaching a security checkpoint.

- **Active Transponders**

A transponder is said to be "active" if it contains its own power source. The active transponder will "ping" its identification periodically and the reader will listen for any transponders in the field. If the active transponder pings quite often it will be heard quickly and detected. The more frequent the ping the faster its battery will expire. If the transponder pings "now and then" there will be some delay until its detected, however the battery will last longer.

The advantage of the active transponder is that it has relatively longer range. This attribute could also be a problem if the range is too great and checkpoints allow passage of a vehicle not even approaching, but just passing by in the area. The disadvantage of active transponders is that they are larger, more costly and have a relatively short battery life. Active transponders may not be a good solution for the detection of vehicles approaching a security checkpoint as the battery life may be less than expected. Active tags are good for asset tracking and personnel tracking, as long as the cost is justified for the tag ($30-$40).

- **Semi-Passive Transponders**

A transponder is said to be "semi-passive" if it contains its own power source used for its internal control circuitry but not used for its transmitter power. Its transmit power will be energy reflected back, or "backscattered", from the reader as it attempts to interrogate it. Here is an analogy that may help in understanding "backscatter".

Two boy scouts are out on a camping trip. One scout stays at the cabin and the other ventures out into the woods. They stay in contact by signaling Morse code between each other using their flashlights. After a few hours of communicating their batteries are dead. This method is analogous to active transponders signaling.

Next, they devise this new scheme to keep communicating without using up batteries so fast. They put this powerful beacon on the roof of the cabin and plug it into the house power. The beacon shines into the woods and signals to the scout on foot. The cabin scout codes his message and then leaves the beacon on steady. The foot scout then decodes the message of the cabin scout and replies by using a hand held mirror reflecting back the cabin beacon's energy. The only energy the scout needed was the small amount of power needed to move the mirror. The light energy was provided by the cabin power.

This technique is known as "semi-passive backscatter". Its advantage over active transponders is relatively lower cost and size and improved battery life. Its advantage over active transponders is improved range.

5. Coding, Modulation

5.1 Coding

Data encoding refers to processing or altering the data bitstream between the time it is retrieved from the RFID chip's data array and its transmission back to the reader. The various encoding algorithms affect error recovery, cost of implementation, bandwidth, synchronization capability, and other aspects of the system design. The most popular methods used in RFID tagging today are the following:

1. **NRZ coding.** A binary 1 is represented by a 'high' signal and a binary 0 is represented by a 'low' signal. NRZ coding is used almost exclusively with FSK or PSK modulation.
2. **Manchester coding.** A binary 1 is represented by a negative transition in the half bit period and a binary 0 is represented by a positive transition. Manchester coding is often used for data transmission form the transponder to the reader based upon load modulation using a subcarrier.
3. **Unipolar RZ coding.** A binary 1 is represented by a 'high' signal during the first half bit period; a binary 0 is represented by a 'low' signal lasting for the entire duration of the bit.
4. **DBP coding.** A binary 0 is coded by a transition of either type in the half bit period; a binary 1 is coded by the lack of a transition. Furthermore, the level is inverted at the start of every bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).
5. **Miller coding.** A binary 1 is represented by a transition of either type in the half bit period; a binary 0 is represented by the continuance of the 1 level over the next bit period. A sequence of zeros created a transition at the start of a bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).
6. **Modified Miller coding.** In this variant of the Miller coding, a 'negative' pulse replaces each transition. Modified Miller coding is highly suitable for use in inductively coupled RFID systems for data transfer from the reader to the transponder. Due to the very short pulse durations ($t_{pulse} << T_{bit}$) it is possible to ensure a continuous power supply to the transponder from the HF field of the reader even during data transfer.
7. **Differential coding.** In differential coding every binary 1 to be transmitted causes a change (toggle) in the signal level, whereas the signal level remains unchanged for a binary zero.
8. **Pulse-pause coding.** In pulse-pause coding (PPC) a binary 1 is represented by a pause of duration t before the next pulse; a binary 0 is represented by a pause of duration 2t before the next pulse. This coding procedure is popular in inductively coupled RFID systems for data transfer from the reader to the transponder. Due to the very short pulse durations ($t_{pulse} << T_{bit}$) it is possible to ensure a continuous power supply to the transponder from the HF field of the reader even during data transfer.

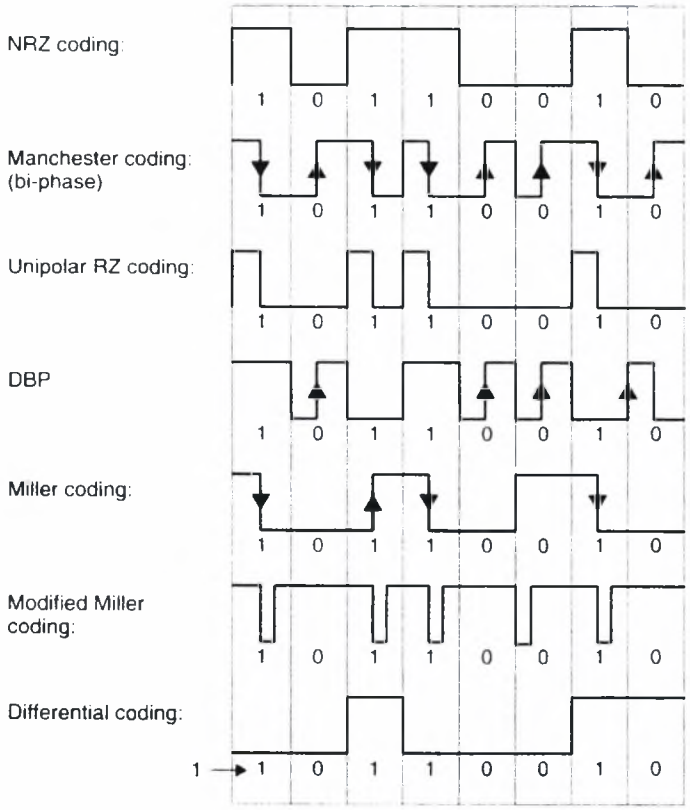

***Figure 5.1*:** Signal coding in RFID systems.

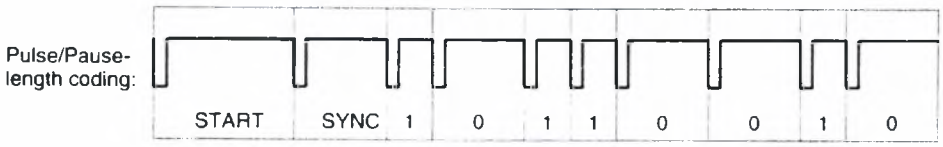

***Figure 5.2*:** Possible signal path in pulse-pause coding.

5.2 Modulation

Although all the data is transferred to the host by amplitude-modulating the carrier (backscatter modulation), the actual modulation of 1's and 0's is accomplished with three additional modulation methods:

1. **ASK (Amplitude Shift Keying).** In ASK modulation, the amplitude of a carrier signal is switched between two states u_0 and u_1 (keying) by a binary code signal. ASK modulation can provide a high data rate but low noise immunity.
2. **FSK (Frequency Shift Keying).** This form of modulation uses two different frequencies for data transfer; the most common FSK mode is Fc/8/10. In other words, a

'0' is transmitted as an amplitude-modulated clock cycle with period corresponding to the carrier frequency divided by 8, and a '1' is transmitted as an amplitude-modulated clock cycle period corresponding to the carrier frequency divided by 10. The amplitude modulation of the carrier thus switches from Fc/8 to Fc/10 corresponding to 0's and 1's in the bitstream, and the reader has only to count cycles between the peak-detected clock edges to decode the data. FSK allows for a simple reader design, provides very strong noise immunity, but suffers from a lower data rate than some other forms of data modulation. In Figure 5.3, FSK data modulation is used with NRZ encoding:

3. **PSK (Phase Shift Keying).** This method of data modulation is similar to FSK, except only one frequency is used, and the shift between 1's and 0's is accomplished by shifting the phase of the backscatter clock by 180 degrees. Two common types of PSK are:

• Change phase at any '0', or

• Change phase at any data change (0 to 1 or 1 to 0).

PSK provides fairly good noise immunity, a moderately simple reader design, and a faster data rate than FSK. Typical applications utilize a backscatter clock of Fc/2, as shown in Figure 5.4.

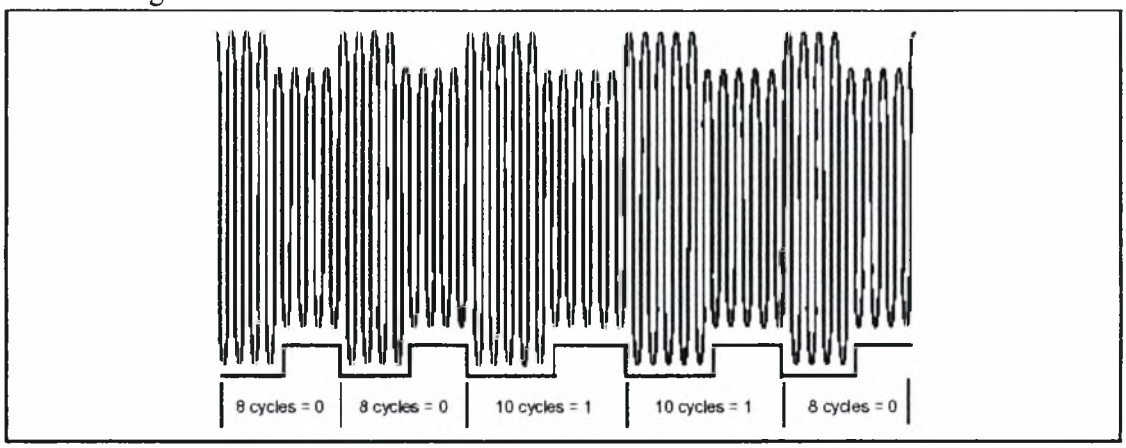

Figure 5.3: FSK modulated signal, Fc/8 = 0, Fc/10 = 1

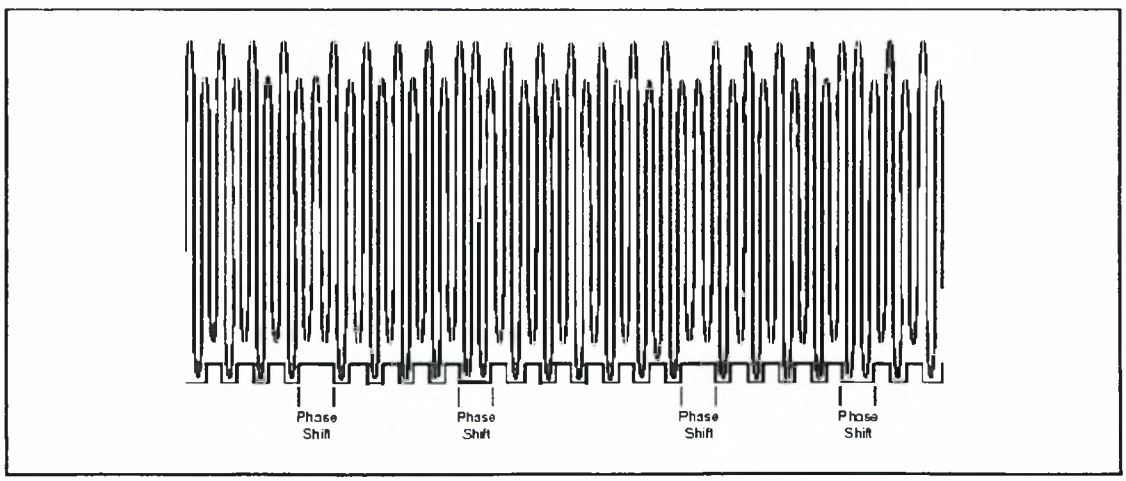

Figure 5.4: PSK modulated signal

6. Anti-collision

Reading or transferring data requires a finite period of time, even if only milliseconds. When a large volume of tags must be read together in the same RF field, the application needs multiplexing and anti-collision features that enable the reader to receive data from each tag. Anti-collision is especially important in applications where a large number of tags are packed tightly together – as on store shelves or in inventory applications (warehouses). Anti-collision methods are usually proprietary since there are no established standards for how this function is to be accomplished.

In general, anti-collision functions are built upon four multiplexing technologies: Space Division Multiple Access (SDMA), Frequency Division Multiplexing (FDMA), Code Division Multiple Access (CDMA) and Time Division Multiplexing (TDMA).

6.1 SDMA

The term *space division multiple access* relates to techniques that reuse a certain resource (channel capacity) in spatially separated areas.

One option is to significantly reduce the range of a single reader, but to compensate by bringing together a large number of readers and antennas to form an array, thus providing coverage of an area. As a result, the channel capacity of adjoining readers is repeatedly made available. Such procedures have been successfully used in large-scale marathon events to detect the run times of marathon runners fitted with transponders. In this application a number of reader antennas are inserted into a tartan mat. A runner travelling over the mat 'carries' his transponder over the interrogation zone of a few antennas that form part of the entire layout. A large number of transponders can thus be read simultaneously as a result of the spatial distribution of the runners over the entire layout.

A further option is to use an electronically controlled directional antenna on the reader, the directional beam of which can be pointed directly at a transponder (adaptive SDMA). So various transponders can be differentiated by their angular position in the interrogation zone of the reader. Phased array antennas are used as electronically controlled directional antennas. These consist of several dipole antennas, and therefore adaptive SDMA can only be used for RFID applications at frequencies above 850 MHz (typical 2.45 GHz) as a result of the size of the antennas. Each of the dipole elements is driven at a certain, independent phase position. The directional diagram of the antenna is found from the different superposition of the individual waves of the dipole elements in different directions. In certain directions the individual fields of the dipole antenna are superimposed in phase, which leads to the amplification of the field. In other directions the waves wholly or partially obliterate each other. To set the direction, the individual elements are supplied with an HF voltage of adjustable, variable phase by controlled phase modifiers. In order to address a transponder, the space around the reader must be

scanned using the directional antenna, until a transponder is detected by the 'search light' of the reader.

A disadvantage of the SDMA technique is the relatively high implementation cost of the complicated antenna system. The use of this type of anticollision procedure is therefore restricted to a few specialised applications.

6.2 FDMA

The term *frequency domain multiple access* relates to techniques in which several transmission channels on various carrier frequencies are simultaneously available to the communication participants.

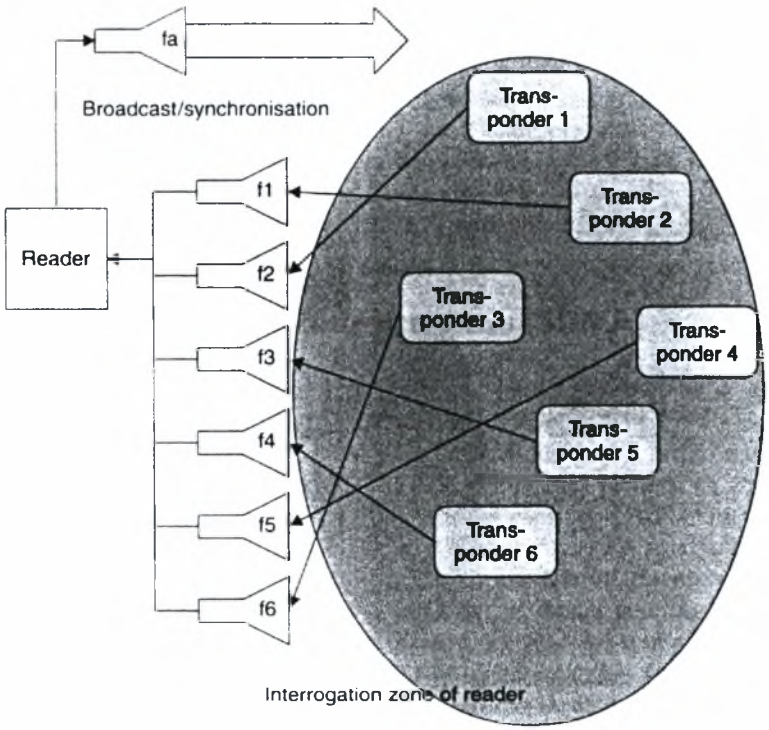

***Figure 6.1*:** In an FDMA procedure several frequency channels are available for the data transfer from the transponders to the reader.

In RFID systems, this can be achieved using transponders with a freely adjustable, anharmonic transmission frequency. The power supply to the transponder and the transmission of control signals (broadcast) takes place at the optimally suited reader frequency f_a. The transponders respond on one of several available response frequencies $f_1 - f_N$ (***figure 6.1***). Therefore, completely different frequency ranges can be used for the

data transfer from and to the transponders (e.g. reader → transponder (downlink): 135 kHz, transponder → reader (uplink): several channels in the range 433 – 435 MHz).

One option for load modulated RFID systems or backscatter systems is to use various independent subcarrier frequencies for the data transmission from the transponders to the reader.

One disadvantage of the FDMA procedure is the relatively high cost of the readers, since a dedicated receiver must be provided for every reception channel. This anticollision procedure, too, remains limited to a few specialized applications.

6.3 CDMA

CDMA employs spread spectrum technology to support multiple and simultaneous accesses. It spreads a data signal to a much wider bandwidth than the original signal. This spreading is done by combining the data signal with a unique code (4.4 trillion codes are available), which is independent of the transmitting data message. In this case, each data signal can be distinguished from many other data signals that are simultaneously transmitted over a common cellular spectrum.

More specifically, using CDMA in RFID systems each data signal generated from a tag is modulated by a pseudo random noise code, which spreads the spectrum of this signal. At the interrogator, the spread signal is coherently demodulated by the same PN code so as to recover the original data signal. CDMA does not require any frame structures to synchronize data transmissions. Therefore, tags are free to concurrently transmit data to the interrogator without any prior resource reservations.

There are two spreading techniques: Direct Sequence (DS) and Frequency Hopping (FH).

6.4 TDMA

The term *time domain multiple access* relates to techniques in which the entire available channel capacity is divided between the participants chronologically. TDMA procedures are particularly widespread in the field of digital mobile radio systems. In RFID systems, TDMA procedures are by far the largest group of anticollision procedures.

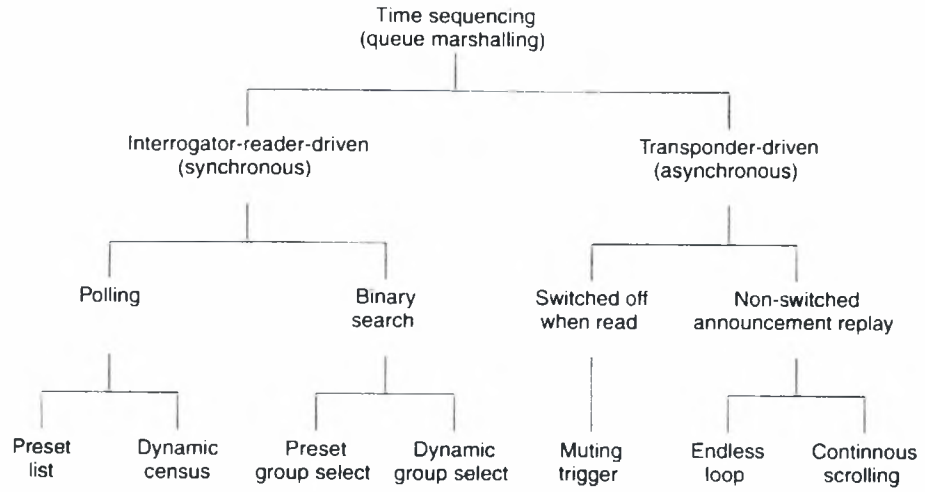

Figure 6.2: Classification of time domain anticollision procedures.

TDMA procedures are differentiated in transponder-driven and interrogator driven procedures (***figure 6.2***):

- ***Transponder-driven procedures*** function asynchronously, since the reader does not control the data transfer. This is the case, for example, in the ALOHA procedure. Transponder-driven procedures are further differentiated in *'switched off'* and *'non-switched'* procedures depending upon whether a transponder is switched off by a signal from the reader after successful data transfer.

- Transponder-driven procedures are naturally very slow and inflexible. Most applications therefore use procedures that are controlled by the reader as the master (***Interrogator-driven procedures***). These procedures can be considered as synchronous, since all transponders are controlled and checked by the reader simultaneously. An individual transponder is first selected from a large group of transponders in the interrogation zone of the reader using a certain algorithm and then the communication takes place between the selected transponder and the reader (e.g. authentication, reading and writing of data). Only then is the communication relationship terminated and a further transponder selected.

  Interrogator-driven procedures are divided into polling and binary search procedures. All these procedures are based upon transponders that are identified by a unique serial number:
  - The *polling procedure* requires a list of all the transponder serial numbers that can possibly occur in an application. The reader interrogates all the serial numbers one after the other, until a transponder with an identical serial number responds. However, this procedure can be very slow, depending upon the number of possible transponders, and is therefore only suitable for applications with few known transponders in the field.

- *Binary search procedures* are the most flexible, and therefore the most common, procedures. In a binary search procedure, a transponder is selected from the group by intentionally causing a data collision in the transponder serial numbers transmitted to the reader following the request command (prompt to the transponders to transmit their serial numbers to the reader in one of the times slots that follow) from the reader. If this procedure is to succeed it is crucial that the reader is capable of determining the precise bit position of a collision using a suitable coding system.

6.5 Example Anticollision Protocols

6.5.1 ALOHA

The simplest of all the multi-access procedures is the *ALOHA* procedure. According to this procedure, as soon as a data packet is available it is sent from the transponder to the reader. This is a transponder-driven stochastic TDMA procedure.

The ALOHA procedure is used exclusively with read-only transponders, which generally have to transfer only a small amount of data (serial numbers), this data being sent to the reader in a cyclical sequence. The data transmission time represents only a fraction of the repetition time, so there are relatively long pauses between transmissions. Furthermore, the repetition times for the individual transponders differ slightly. There is therefore a certain probability that two transponders can transmit their data packets at different times and the data packets will not collide with one another.

6.5.2 Slotted ALOHA

In this procedure, transponders may only begin to transmit data packets at defined, synchronous points in time (slots). The synchronisation of all transponders necessary for this must be controlled by the reader. This is therefore a stochastic, interrogator-driven TDMA anticollision procedure.

In order to synchronise and control the transponders, a set of commands like that in figure 6.3 is defined.

Command	Description
REQUEST	Synchronises all transponders in the reader's interrogation zone and prompts the transponders to transmit their serial numbers to the reader in one of the time slots that follow.
SELECT(SNR)	Sends a (previously determined) serial number (SNR) to the transponder as a parameter. The transponder with this serial number is thereby cleared to perform read and write commands (selected). Transponders with a different serial number continue to react only to a REQUEST command.

READ_DATA	The selected transponder sends stored data to the reader. (In a real system there are also commands for writing, authentication, etc.)

Figure 6.3: Command set for anticollision.

A reader in wait mode transmits a REQUEST command at cyclical intervals. As soon as the transponders have recognised the REQUEST command, each transponder selects one of the available slots by means of a random-check generator, in order to send its own serial number to the reader.

If a serial number is read without errors, then the detected transponder can be selected by the transmission of a SELECT command and then read or written without further collisions with other transponders. If no serial number were detected at the first attempt the REQUEST command is simply repeated cyclically.

When the previously selected transponder has been processed, further transponders in the interrogation zone of the reader can be sought by means of a new REQUEST command.

A form of slotted ALOHA (named Slotted ALOHA/TDMA) has been proposed in paper [23]. The Slotted ALOHA/TDMA protocol uses a three-phase cyclic frame structure to synchronize the various activities within a frame duration (frames are transmitted continuously and contiguously): Message Control Phase, Data Transfer Phase and Selection Phase. Also, let each frame contain 4 message slots and 16 ALOHA slots.

In *the Message Control Phase*, an interrogator will assign a maximum of 4 tag requests to the available message slots. These assignments are based on the reserved ALOHA slots from the previous frame. Tag IDs extracted from these ALOHA slots are inserted into a frame control message (FCM). The corresponding tags will be acknowledged via this FCM.

When a tag finds its ID in the FCM, it can use the assigned message slot to transmit data to the interrogator in the *Data Transfer Phase* of the current frame. Those who cannot find their IDs will select another ALOHA slot in the Selection Phase. Interrogator sends positive acknowledgement messages to tags when their data messages are successfully received. Otherwise negative acknowledgement messages are sent.

In the *Selection Phase*, each active tag randomly selects one of the ALOHA slots and sends its ID in a tag-ID message to the interrogator. Since slotted ALOHA/TDMA allows many tags to make the selections simultaneously, collisions often occur at the interrogator. In this case the interrogator will not assign message slots to these tags. Good tag IDs are inserted into the appropriate ALOHA slots to be processed in the next MessageControl Phase.

Tags and an interrogator interact by means of FCMs, data messages, acknowledgement messages, and tag-ID messages. Guard bands are introduced to prevent tags from transmitting data between frames. A tag can transmit data to the interrogator when a message slot is assigned from the FCM.

It must be mentioned that it is not necessarily the case that there will be a data collision if several data packets are sent at the same time: if one transponder is closer to the reader than the others, that transponder may be able to override the data packets from other transponders as a result of the greater signal strength at the reader. This is known as the *capture effect*.

6.5.3 Tree-Walking Singulation Algorithm

The tree-walking singulation algorithm, proposed in paper [24], enables an RFID reader to identify the serial numbers of nearby tags individually by means of a bit-by-bit query process resembling a depth-first search of a binary tree. The tree-walking singulation algorithm is a binary search TDMA procedure.

Suppose the tags in a given system bear unique identifiers of some fixed bit-length k (such as k = 64, 96, or 128). Let || denote the concatenation operator for bit strings. The set of all possible k-bit identifiers can be viewed as the leaves of a standard binary tree of depth k. The root of this tree has depth 0 and is labeled with the empty string. A node of depth d is labeled with a binary string x of length d; if d < k, then the node has two children at depth d+1: a "left child" with label x0, and a "right child" with label x1. (Here x0 means x || 0 and x1 means x || 1). We regard the branches of a given node in this tree as bearing labels '0' and '1', respectively associated with the left and right branches. Thus, a node at depth d in this tree may be uniquely identified by a binary prefix B = b1b2 . . . bd, representing the sequence of branch labels of branches traversed in a path from the root to the node. It follows that each of the 2^k leaves in the tree has a unique associated k-bit string. We view each such leaf as representing a distinct possible tag serial number.

The tree-walking algorithm is a recursive depth-first search performed by a reader in the following way. Let the subtree of a node denote all its descendents in the tree. The reader initiates the tree-walking algorithm at the root of the tree. Starting at a given node B = b1b2 . . . bd, the reader queries all tags bearing serial numbers in the leaves of the corresponding subtree, i.e., all tags whose serial numbers bear the prefix B; all other tags are instructed to remain silent. The queried tags reply to the reader with the d+1-st bit in their serial numbers; i.e., each tag broadcasts a '0' if it lies in the left subtree of the node B, and a '1' if it lies in the right subtree. Consequently, if there are tags in both the left and right subtrees of B, then the tags together simultaneously broadcast both a '0' and a '1', creating a collision in the broadcast bit. In this case, when a collision is detected, the reader recurses (sequentially in turn) beginning at its child nodes B || 0 and B || 1. If, on the other hand, the tags all reply with only a single bit b, i.e., they all lie in the same subtree, then the reader recurses on the node B || b, and ignores the other (empty) subtree. When the algorithm reaches a leaf (at depth k), it outputs the associated k-bit sequence, which is the serial number of the tag just read. The full output of the algorithm is a list of the ID numbers of all tags within range.

The running time of this algorithm is bounded by the product of k and the number of tags being read. In practice, a shopping cart full of goods should be scannable in a few seconds.

7. Frequencies

7.1 Overview

Because RFID systems generate and radiate electromagnetic waves, they are justifiably classified as radio systems. The function of other radio services must under no circumstances be disrupted or impaired by the operation of RFID systems. It is particularly important to ensure that RFID systems do not interfere with nearby radio and television, mobile radio services (police, security services, industry), marine and aeronautical radio services and mobile telephones.

The need to exercise care with regard to other radio services significantly restricts the range of suitable operating frequencies available to an RFID system. For this reason, it is usually only possible to use frequency ranges that have been reserved specifically for industrial, scientific or medical applications or for short range devices. These are the frequencies classified worldwide as ISM frequency ranges (Industrial-Scientific-Medical) or SRD frequency ranges, and they can also be used for RFID applications.

Frequency ranges for RFID-Systems

Frequency range	Comment	Allowed fieldstrength / transmission power
< 135 kHz	low frequency, inductive coupling	72 dBµA/m
6.765 .. 6.795 MHz	medium frequency (ISM), inductive coupling	42 dBµA/m
7.400 .. 8.800 MHz	medium frequency, used for EAS (electronic article surveilance) only	9 dBµA/m
13.553 .. 13.567 MHz	medium frequency (13.56 MHz, ISM), inductive coupling, wide spread usage for contactless smartcards (ISO 14443, MIFARE, LEGIC, ...), smartlabels (ISO 15693, Tag-It, I-Code, ...) and item management (ISO 18000-3).	42 dBµA/m
26.957 .. 27.283 MHz	medium frequency (ISM), inductive coupling, special applications only	42 dBµA/m
433 MHz	UHF (ISM), backscatter coupling, rarely used for RFID	10 .. 100 mW
868 .. 870 MHz	UHF (SRD), backscatter coupling, new frequency, systems under developement	500 mW, Europe only
902 .. 928 MHz	UHF (SRD), backscatter coupling, several systems	4 W - spread spectrum, USA/Canada only
2.400 .. 2.483	SHF (ISM), backscatter coupling, several	4 W - spread spectrum,

GHz	systems, (vehicle identification: 2.446 .. 2.454 GHz)	USA/Canada only, 500 mW, Europe
5.725 .. 5.875 GHz	SHF (ISM), backscatter coupling, rarely used for RFID	4 W USA/Canada, 500 mW Europe

Figure 7.1: Frequency ranges for RFID systems

The following table shows an overview of RFID performances at various frequencies:

	LF	**HF**	**UHF**	**Microwave**
Frequency Range	< 135 kHz	10..13.56 MHz	850..950 MHz	2.5..5.8 GHz
Read Range	~10 cm	~1 m	2 – 5 m	~1 m
Coupling	Inductive	Inductive	Backscatter	Backscatter
Application	Smart Card, Ticketing, Anti-theft, Animal tagging	Small Item Management, Anti-theft, Supply Chain	Transportation, Vehicle ID, Access/Security, Large Item Management, Supply Chain	Transportation, Vehicle ID, Access/Security, Large Item Management, Supply Chain

Figure 7.2: RFID performances at various frequencies

7.2 Characteristics of the frequency ranges

7.2.1 Low Frequency (LF) (<135 KHz)

Low Frequency (LF) RFID is typically defined by radio frequency transponder devices operating in the frequency range of 100 kHz to 140 kHz. Typical frequencies are 125 kHz and 134 kHz. The transponders are usually passive, read-only, or read-write transponders.

The advantage of LF RFID is that it is less susceptible to the effects of nearby metals and liquids as compared to devices operating at higher frequencies (i.e. HF-13.56 mHz, UHF-900 mHz). It is for this reason that the U.S. Fisheries Department uses LF RFID to track fish in streams and major car retailers use LF to inventory automobiles. LF has been available for the past 20 years and continues to be the favorite RFID solution for many applications. Contrary to popular belief, LF has not been replaced by higher frequencies and may never become obsolete due to its robust properties. Other advantages of LF are that it is widely used and has been used for many years and that transponders can be more compact in certain cases (i.e. glass transponders).

The disadvantages of LF are the fact that, usually, only one transponder can be read at a time (only one transponder can be in the reading field at a time), the read ranges are shorter and the transponders are generally more expensive and typically bulkier than HF tags, as well as the memory capacity of LF transponders is generally lower than HF tags.

7.2.2 High Frequency (HF) (13.56 MHz)

The High Frequency RFID devices available today typically operate at 13.56 MHz. The original devices developed as HF RFID were known as MIFARE and I-Code from Philips Semiconductor and Tag-it from Texas Instruments. Although these devices all operated on a center frequency of 13.56 MHz their air interface protocols and data structures were totally incompatible with each other. In 1999 and 2000, Philips and TI agreed to share some of their intellectual property and create the ISO 15693 "Vicinity" card standard and the ISO 14443 "Proximity" card standard. These ISO "specs" currently define the HF RFID smart card and smart label components.

HF RFID devices work on magnetic wave coupling principles, similar to that of primary-secondary windings in transformers, not as conventional radio wave theory, as we know it. HF RFID Readers are matched to loop antennas that convert time-varying electrical current into the magnetic radiation field pattern. Nearby HF tags that are in the field get a current induced in their winding and it is this induced current that provides power for the passive chip to operate.

High Frequency RFID transponders are typically passive, read-only, read-write, or WORM (write once, read many) transponders. Similar to LF transponders, they provide good penetration through non-conductive materials and nonconductive liquids. They are less expensive than inductive LF transponders and they have relatively short read ranges and slow data rates when compared to higher frequencies used with contactless smart cards.

High Frequency RFID devices have anti-collision intelligence that allows hundreds of tags to operate concurrently in the same antenna field. They are well suited for applications that do not require long reading range of multiple transponders as well as for higher transponder-to-reader ratio applications.

7.2.3 Ultra-High Frequency (UHF) (868 MHz to 915 MHz)

The Ultra High Frequency, UHF RFID passive devices that are available today typically operate in the band of 860 – 960 MHz. The United States has specified 915 MHz while the European Union has specified 868 MHz for UHF RFID applications.

UHF RFID transponders are typically active and passive, read-only, read-write, or WORM transponders. They are less expensive than LF and HF transponders and they

provide good penetration through non-conductive materials and non-conductive liquids. UHF frequencies offer higher range capability, higher data transfer rates, and faster identification compared to lower frequencies. It could be said that UHF frequencies provide a good balance between range and performance, especially for multiple transponder reading.

7.2.4 Microwave (2.45 GHz, 5.8 GHz)

Certain types of RFID devices are well suited to operate at microwave frequencies. The microwave portion of the electromagnetic spectrum is defined from 1600 MHz to 30,000 MHz (or 1.6 GHz to 30 GHz).

Microwave RFID devices typically operate in "semi-passive mode". That is a mode that is somewhere in between passive, self-powered, transponders and battery operated active tags. They have similar characteristics to UHF transponders, but faster read rates. Their cost is often twice as much or more than lower frequencies. They provide good penetration through non-conductive materials and they offer the most directional signal. Their signal is absorbed by water and water-based solutions and reflected by metals and other conductive surfaces.

8. Standards

RFID technology is associated to standards and regulations, designed to ensure safe operation with respect to other electrical and radio equipment, and guarantee interoperability between different manufacturers' readers and tags. Two main organizations have set the rules for RFID systems: these are ISO (International Standards Organization) and EPC (Electronic Product Code) Global.

Currently, efforts are under way for merging the ISO and the EPC Global into a unique standard which will ensure the widespread adoption and high volumes of RFID tags within the supply chain, the transportation, the biomedical applications etc.

8.1 The ISO series

ISO defines the Air interface communication between Reader->Tag and Tag->Reader and include parameters like Communication protocol, Signal Modulation types, Data coding and frames, Data Transmission rates and Anti-collision (detection and sorting of many tags in the Reader field at the same time). An introduction to the standards for various applications is presented in the following sections.

8.1.1 Animal Identification

ISO standards 11784, 11785, 14223 deal with the identification of animals using RFID systems.

- ISO 11784: 'Radio-frequency identification of animals – Code structure'
- ISO 11785: 'Radio-frequency identification of animals – Technical concept'
- ISO 14223: 'Radio-frequency identification of animals – Advanced transponders'
  Part 1: Air interface
  Part 2: Code and command structure
  Part 3: Applications

The constructional form of the transponder used is not specified in the standards and therefore the form can be designed to suit the animal in question.

8.1.2 Contactless smart cards

There are currently three different standards for contactless smart cards based upon a broad classification of the range:

Standard	Card Type	Approximate range
ISO 10536	Close Coupling	0 – 1 cm
ISO 14443	Proximity coupling	0 – 10 cm
ISO 15693	Vicinity coupling	0 – 1 m

Most of the standard for close coupling smart cards – ISO 10536 – had already been developed by between 1992 and 1995. Due to high manufacturing costs of this type of card and the small advantages in comparison to contact smart cards, close coupling systems were never successful on the market and today they are hardly ever used.

8.1.3 Data Carriers for Tools and Clamping Devices

The ISO 69873 standard specifies the dimensions for contactless data carriers and their mounting space in tools and cutters. Normally the data carriers are placed in a quick release taper shaft in accordance with ISO 69871 or in a retention knob in accordance with ISO 69872 (installation examples are given in each standard).

8.1.4 Container Identification

The ISO 10374 standard describes an automatic identification system for containers based upon microwave transponders. The optical identification of containers is described in ISO 6346 and is reflected in the data record of the transponder-based container identification.

8.1.5 Item Management

The complete ISO standard list for item management in RFID systems is the following:

Standard Code	Description
ISO 15961	RFID for Item Management: Host Interrogator: Tag functional commands and other syntax features
ISO 15962	RFID for Item Management: Data Syntax
ISO 15963	Unique Identification of RF tag and registration authority to manage the uniqueness
ISO 18000	RFID for Item Management: Air Interface -1 Generic parameters -2 below 135 kHz -3 at 13.56 MHz -4 at 2.45 GHz -5 at 5.8 GHz -6 at UHF frequency band

Figure 8.1: ISO standard list for item management in RFID systems

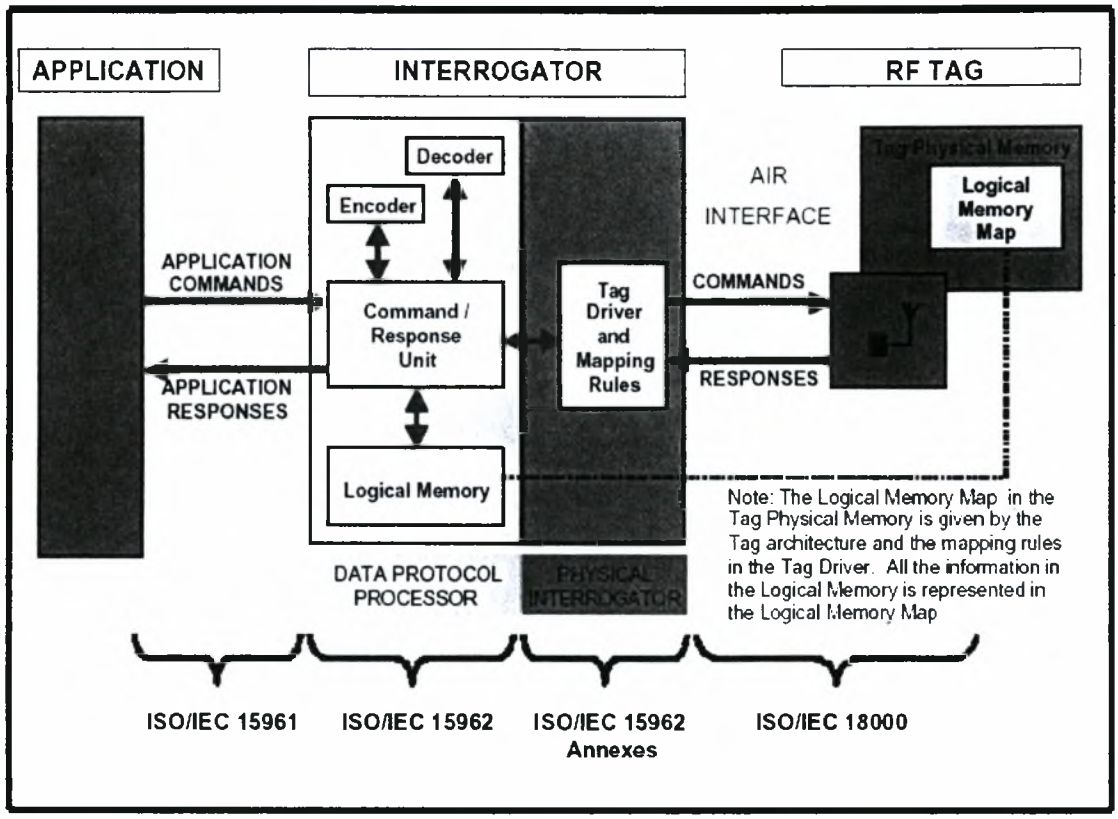

Figure 8.2: ISO standard list for item management in RFID systems illustrated

8.2 The EPC – Electronic Product Code

One of the key elements of the current RFID based technology, which aims to improve supply chain efficiency and reduce operating costs, is the EPC (Electronic Product Code).

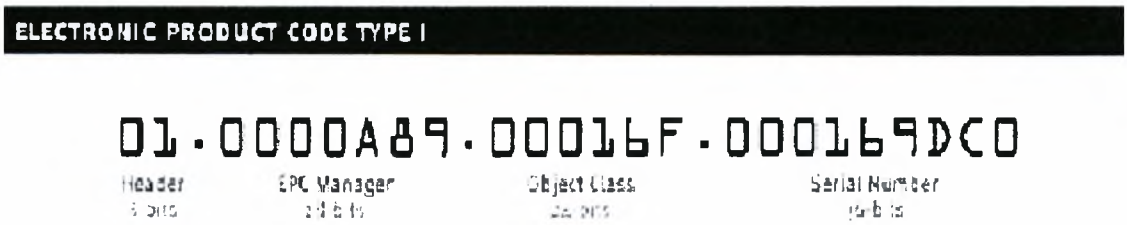

Figure 8.3: Electronic Product Code

The code is similar to the UPC (Universal Product Code) used in bar codes, and ranges from 64 bits to 256 bits. The main difference between EPC and bar codes is its serial number which allows distinguishing the uniqueness of an item and tracking it through the supply chain. The organization which defines the EPC requirements is EPC Global. EPC Global is going to issue a new revision to overcome this standards non-uniformity. The definition of a second-generation EPC air interface standard (formerly known as Class 1 Generation 2 or Class 1 Gen 2) which EPC Global has renamed the UHF Generation 2 Foundation Protocol, is expected for September 2004. The UHF Generation 2 Foundation Protocol will also form the basis for EPC Global's plans to have its work incorporated into an ISO standard.

8.2.1 EPC Tag Classes

EPC Global distinguishes RFID tags in 5 classes, according to their read and write capabilities:

- ***CLASS 0 (READ ONLY)*** Factory programmed

These are the simplest type of tags, where the data, which is usually a simple ID number (EPC), is written only once into the tag during manufacture (no update is possible). Class 0 is also used to define a category of tags called EAS (electronic article surveillance used for anti-theft devices), which have no ID, and only announce their presence when passing through an antenna field.

- ***CLASS 1 (WRITE ONCE READ ONLY)*** Factory or User programmed

In this case the tag is manufactured with no data written into the memory. Data can then either be written by the tag manufacturer or by the user – one time. After this no further update is possible and the tag can only be read. Tags of this type are usually used as simple Identifiers.

- ***CLASS 2 (READ/WRITE)***

These tags allow users to both read and write data into the tags memory. They are typically used as data loggers, and therefore contain more memory space than tags which carry only simple ID numbers.

- ***CLASS 3 (READ/WRITE)*** with on board sensors

These tags are just like CLASS 2 plus containing on-board sensors for recording parameters like temperature, pressure etc., which are recorded into the tags memory. As sensor readings must be loaded into memory in absence of the reader, the tags are either semi-passive or active, thus requiring an on-board power source.

- ***CLASS 4 (READ/WRITE)*** with integrated transmitters

These tags are just like radio devices that can communicate with other tags and devices also in absence of the reader. This means that they are completely active and have their own on-board power source.

Class	Known as	Memory	Power Source	Application
0	EAS | EPC [1]	None | EPC	Passive	Ant-theft | ID
1	EPC	Read -Only	Any	Identification
2	EPC	Read-Write	Any	Data logging
3	Sensor Tags	Read-Write	Semi-Passive/Active	Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc networking

[1] The section on EPC standards evolution shows that the EPC class 0 is likely to evolve to a read-write

Figure 8.4: Different tag classes

9. Privacy

RFID has given rise to many privacy fears. According to privacy advocates, marketers and retailers can develop detailed profiles of their customers, based on their own records of transactions with an individual as well as on that individual's transactions with other institutions with help of RFID. Even when these databases contain only transactional data, such as name, address and product or service used or inquired about, they serve as the basic source for development of detailed profiles by interconnecting each other, now very easily with help from ubiquitous RFID.

RFID tags can be attached without knowledge of consumer and this is major concern for privacy advocacy groups. According to them, consumer privacy is enhanced when consumers are aware of information practices and are given a choice over information provision and use. In contrast, consumer privacy is decreased when there is unwanted marketing contact or information gathering without consent.

Some of the approaches suggested for protecting consumer privacy threatened by RFID tags are discussed below. No single approach is likely to be completely satisfactory, however; a combination of methods may prove to be best.

a) The "Kill Tag" approach
The most straightforward approach for the protection of consumer privacy is to "kill" RFID tags before they are placed in the hands of consumers. A killed tag is truly dead and can never be re-activated.

The standard mode of operation proposed by the Auto-ID Center is indeed for tags to be killed upon purchase of the tagged product. When this design is incorporated a tag can be killed by sending a special kill command (including a short 8-bit password). For example, a supermarket might use RFID tags to facilitate inventory management and monitoring of shelf stocks. To protect consumer privacy, checkout clerks would kill the tags of purchased goods; no purchased goods would contain active RFID tags.

From the privacy advocates perspective the "kill" approach is inadequate. According to them, there are many situations and many environments in which simple measures like kill commands are unworkable or undesirable for privacy enforcement as there are many times customer him/herself would not want to kill for specific products e.g., when he/she has got a microwave oven that reads cooking instructions from food packages which rely on actively operational tags.

b) The Faraday Cage approach
An RFID tag may be shielded from scrutiny using what is known as a Faraday Cage, a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies).

Although this approach is valuable in some cases, e.g. foil-lined wallets could be used to carry high-value currency notes supplied with active RFID tags, there is a vast range of

objects using RFID tags that cannot be placed conveniently in containers, such as clothing, wrist-watches and cell phones. Faraday cages thus represent at best a very partial solution to consumer privacy.

c) The Active Jamming approach

Active jamming of RF signals is another, related physical means of shielding tags from view. The consumer could carry a device that actively broadcasts radio signals so as to block and/or disrupt the operation of any nearby RFID readers.

This approach may be illegal – at least if the broadcast power is too high – and could cause severe disruption of all nearby RFID systems, even those in legitimate applications where privacy is not a concern.

d) The Smart RFID Tag approach

Another general approach is to make the RFID tags smarter, so that they interact in a way that protects privacy better, while providing the desired active functionality would typically involve the use of cryptographic methods.

In smart RFID approach, consumers can selectively block readers from reading any chip on the consumer's person. Such blocker chips can be built cheaply. They only need to interfere with the "singulation" protocol that readers use to address each RFID chip individually in turn.

By giving consumers the ability to block unwanted readers form reading their RFID tags, as well as allowing consumers to "kill" their RFID tags, one may be able to provide consumers with sufficient control over how their RFID tags are used to allow implementation of acceptable privacy policies.

e) The Regulation approach

Unlike the above approaches, this approach doesn't rely on technology. Simson Garfinkel of MIT Auto-ID proposed the "RFID Bill of Rights", a set of principles that consist of five articles as a voluntary framework for commercial deployment of RFID tags. According to these articles, consumers should have:

1. The right to know whether products contain RFID tags.
2. The right to have RFID tags removed or deactivated when they purchase products.
3. The right to use RFID-enabled services without RFID tags.
4. The right to access an RFID tag's stored data.
5. The right to know when, where and why the tags are being read.

10. Active and Passive RFID Comparison

10.1. Technical Characteristics of Active and Passive RFID

Although they both fall under the "RFID" moniker and are often discussed interchangeably, Active RFID and Passive RFID are fundamentally different technologies. While both use radio frequency energy to communicate between a tag and a reader, the method of powering the tags is different. Active RFID uses an internal power source (battery) within the tag to continuously power the tag and its RF communication circuitry, whereas Passive RFID relies on RF energy transferred from the reader to the tag to power the tag.

While this distinction may seem minor on the surface, its impact on the functionality of the system is significant. Passive RFID either 1) reflects energy from the reader or 2) absorbs and temporarily stores a very small amount of energy from the reader's signal to generate its own quick response. In either case, Passive RFID operation requires very strong signals from the reader, and the signal strength returned from the tag is constrained to very low levels by the limited energy. On the other hand, Active RFID allows very low-level signals to be received by the tag (because the reader does not need to power the tag), and the tag can generate high-level signals back to the reader, driven from its internal power source. Additionally, the Active RFID tag is continuously powered, whether in the reader field or not. These differences impact communication range, multi-tag collection capability, ability to add sensors and data logging, and many other functional parameters.

	Active RFID	**Passive RFID**
Tag Power Source	Internal to tag	Energy transferred from the reader via RF
Tag Battery	Yes	No
Availability of Tag Power	Continuous	Only within field of reader
Required Signal Strength from Reader to Tag	Low	High (must power the tag)
Available Signal Strength from Tag to Reader	High	Low

Figure 10.1: Technical differences between Active and Passive RFID technologies.

10.2. Functional Capabilities of Active and Passive RFID

Because of the technical differences outlined above, the functional capabilities of Active and Passive RFID are very different and must be considered when selecting a technology for a specific application.

i. Communication Range

For Passive RFID, the communication range is limited by two factors: 1) the need for very strong signals to be received by the tag to power the tag, limiting the reader to tag range, and 2) the small amount of power available for a tag to respond to the reader, limiting the tag to reader range. These factors typically constrain Passive RFID operation to 3 meters or less. Depending on the vendor and frequency of operation, the range may be as short as a few centimeters. Active RFID has neither constraint on power and can provide communication ranges of 100 meters or more.

ii. Multi-Tag Collection

As a direct result of the limited communication range of Passive RFID, collecting multiple collocated tags within a dynamic operation is difficult and often unreliable. An example scenario is a forklift carrying a pallet with multiple tagged items through a dock door. Identifying multiple tags requires a substantial amount of communication between the reader and tags, typically a multi-step process with the reader communicating individually with each tag. Each interaction takes time, and the potential for interference increases with the number of tags, further increasing the overall duration of the operation. Because the entire collection operation must be completed *while the tags are still within the range of the reader*, Passive RFID is constrained in this aspect. For example, one popular Passive RFID systems available today requires more than 3 seconds to identify 20 tags. With a communication range of 3 meters, this limits the speed of the tagged items to less than 3 miles per hour.

Active RFID, with operating ranges of 100 meters or more, is able to collect thousands of tags from a single reader. Additionally, tags can be in motion at more than 100 mph and still be accurately and reliably collected.

iii. Sensor Capabilities

One functional area of great relevance to many supply chain applications is the ability to monitor environmental or status parameters using an RFID tag with built-in sensor capabilities. Parameters of interest may include temperature, humidity, and shock, as well as security and tamper detection. Because Passive RFID tags are only powered while in close proximity to a reader, these tags are unable to continuously monitor the status of a sensor. Instead, they are limited to reporting the current status when they reach a reader. Active RFID tags are constantly powered, whether in range of a reader or not, and are therefore able to continuously monitor and record sensor status, particularly valuable in measuring temperature limits and container seal status. Additionally, Active RFID tags can power an internal real-time clock and apply an accurate time/date stamp to each recorded sensor value or event.

iv. Data Storage

Both Active and Passive RFID technologies are available that can dynamically store data within the tag. However, because of power limitations, Passive RFID typically only provides a small amount of read/write data storage, on the order of 128 bytes (1000 bits) or less, with no search capability or other data manipulation features. Larger data storage and sophisticated data access capabilities require the tag to be powered for longer periods of time and are impractical with Passive RFID. Active RFID has the flexibility to remain powered for access and search of larger data spaces, as well as the ability to transmit longer data packets for simplified data retrieval. Active RFID tags are in common use with 128K bytes (1 million bits) of dynamically searchable read/write data storage.

	Active RFID	**Passive RFID**
Communication Range	Long range (100m or more)	Short or very short range (3m or less)
Multi-Tag Collection	• Collects 1000s of tags over a 7 acre region from a single reader • Collects 20 tags moving at more than 100 mph	• Collect's hundreds of tags within 3 meters from a single reader • Collects 20 tags moving at 3 mph^2 or slower.
Sensor Capability	Ability to continuously monitor and record sensor input; data/time stamp for sensor events	Ability to read and transfer sensor values only when tag is powered by reader; no date/time stamp
Data Storage	Large read/write data storage (128KB) with sophisticated data search and access capabilities available	Small read/write data storage (e.g. 128 bytes)

Figure 10.2: Summary of functional capabilities of Active and Passive RFID technologies.

minute variations in the seal position or integrity and implementing sophisticated anti-spoofing techniques. Immediately upon detection of a problem, the date and time and event code can be logged in the tag's memory, providing a complete audit trail of all events during the shipment.

iv. Electronic Manifest

For supply chain applications where there is a need to store an electronic manifest within the tag, such as customs inspection, only Active RFID is an appropriate option. Passive RFID does not provide sufficient data storage or data search capabilities.

A key consideration in any implementation of RFID is the impact on business processes. Clearly, the objective is to minimize these impacts, but they are virtually impossible to eliminate completely. As a general rule, Active RFID requires significantly fewer changes to existing business processes than Passive RFID. There are several reasons for this: 1) Passive RFID has a very limited read range, requiring tagged assets and items to move along well-defined paths and past specific read points, 2) Passive RFID has limited multi-tag collection capabilities, requiring large groupings of tagged items to be dispersed before passing a read point, and 3) Passive RFID is unable to read tags moving at high speed3. The result is that Passive RFID may require substantial process re-design and worker training to be effectively implemented. The costs associated with business process re-engineering must be considered, along with the costs of software, tags, and readers, when assessing the total cost of implementation and ownership of an RFID system.

	Active RFID	**Passive RFID**
Area Monitoring (e.g. warehouse, terminal, yard)	**Yes**	**No**
High-Speed, Multi-Tag Portal	**Yes**	**Limited**
Cargo Security Applications	**Sophisticated** (continuous tamper detection, anti-spoofing techniques, date/time stamp)	**Simple** (one-time tamper event detection, no time stamp, susceptible to "spoofing")
Electronic Manifest	**Yes**	**No**
Business Process Impacts	**Minimal**	**Substantial**
Application Characteristics	∝ Dynamic business process ∝ Unconstrained asset movement ∝ Security / sensing ∝ Data storage / logging	∝ Rigid business process ∝ Constrained asset movement ∝ Very simple security / sensing ∝ Limited data storage

Figure 10.3: Applicability of Active and Passive RFID technologies to supply chain visibility.

11. Applications

11.1 RFID Benefits

Given the robust tracking capability relative to bar coding, RFID is capable of offering significant incremental benefits associated with operational improvement and market intelligence. An AMR research study indicates that tracking with RFID can generate a 20% reduction in warehousing labor, a 25% reduction in inventory and a 3%-4% increase in sales versus current tracking technologies. The following highlight how RFID can achieve these benefits.

Greater Labor Savings – The increased reading capability reduces the need for manual intervention as RFID readers can automatically scan incoming shipments entering a distribution center or retail location. RFID's more robust scanning capability also reduces labor associated with pallet breakdown and cross docking activities. In addition, improved inventory accuracy also reduces the need for laborintensive physical counts.

Improved Inventory Management – RFID's faster scanning process significantly increases inventory visibility, which enables better inventory management through more efficient staging and rapid cross docking. Improved inventory management increases inventory velocity and allows for incremental labor cost reductions. Further, as a result of the enhanced tracking, less safety stock is required.

Better Supply Chain Communication – As supply chain members receive better, faster and more accurate inventory information, they improve their forecasting and plan their operations more effectively. As a result, retailers have fewer stock outs, resulting in improved sales (retail sales are said to be reduced by nearly 4% each year from stock outs), while distribution centers save through increased shipping accuracy, which lowers returns and improves customer satisfaction.

Retail/Manufacturer Protections – Because RFID is capable of tracking specific items, recall items can be rapidly identified, providing strong consumer protection and reducing recall costs. Item tracking capability can also reduce the incidence of counterfeit products.

Advanced Market/Customer Intelligence – Bar code technology, combined with data warehousing systems, has increased retailers' capability to understand customer purchasing practices, and thus allowing for a more targeted approach to sales and marketing campaigns. Because of the increased in-store tracking capabilities offered by RFID, it is believed that this type of intelligence will increase significantly.

11.2 RFID Applications

The main features of radio frequency tagging are ability to identify objects without a clear line of sight between tag and reader, read/write capability, and cluster reading.

✓ **Identification without visual contact**

People, items, and cartons can be identified even if material comes between the reader and the tag.

✓ **Read/write**
Unlike barcode identification technology, certain RFID tags can store data, allowing system designers to place "handling codes" directly on the object as it travels through a system.
✓ **Cluster reading**
Specially-designed readers can read many tags at once, increasing the throughput of automated accounting procedures.

These features determine the applications of RFID technology. The most important applications of the RFID technology will be presented in the following sections.

11.2.1 TRANSPORTATION/DISTRIBUTION

a. Fare systems using electronic payment
Transport association regions are often divided into different fare zones and payment zones. There are also different types of travel pass, time zones and numerous possible combinations. The calculation of the fare can therefore be extremely complicated in conventional payment systems and can even be a source of bewilderment to local customers.

Electronic fare management systems, on the other hand, facilitate the use of completely new procedures for the calculation and payment of fares. There are four basic models for electronic fare calculation:

- ***Fare system 1***
  Payment takes place at the beginning of the journey. A fixed amount is deducted from the contactless smart card the passenger carries, regardless of the distance traveled.
- ***Fare system 2***
  At the beginning of the journey the entry point (check-in) is recorded on the contactless smart card. Upon disembarking at the final station (check-out), the fare for the distance traveled is automatically calculated and deducted from the card. In addition, the card can be checked at each change-over point for the existence of a valid 'check-in' entry. To foil attempts at manipulation, the lack of a 'check-out' record can be penalized by the deduction of the maximum fare at the beginning of the next journey.
- ***Fare system 3***
  This model is best suited for interlinked networks, in which the same route can be traveled using different transport systems at different fares. Every time the passenger changes vehicles a predetermined amount is deducted from the card, bonus fares for long distance travelers and people who change several times can be automatically taken into account.
- ***Best price calculation***
  In this system all journeys made are recorded on the contactless card for a month. If a certain number of journeys was exceeded on one day or in the month as a whole, then the contaless card can automatically be converted into a cheaper 24 hour or montly card. This gives the customer maximum flexibility and the best possible fares. Best

price calculation improves customer relations and makes a big contribution to customer satisfaction.

b. Toll Road Control
The goal in toll road control systems is to electronically identify vehicles passing a toll station and to debit their accounts automatically for using the toll road without impeding traffic flow.

11.2.2 INDUSTRIAL

a. Production process
Production processes underwent a process of continuous rationalisation during the development of industrial mass production. This soon led to production line assembly ('conveyor belt production'), with the same stage of production being performed at a certain position on the assembly line time after time. For the present, a production process of this type is only able to produce objects that are identical in function and appearance.

If different variants of a product are to be produces at the same time on an assembly line in an automated procedure, the object must be identified and its status clearly recognised at every work station, so that the correct processes can be performed. Originally, this was achieved by objects being accompanied by process cards, which gave the operating personnel all the information required at a particular workstation – the desired colour, for example. RFID technology now provides an additional option – data carriers that can not only be read, but also written. Now, in addition to recording the identity of an object, it is also possible to document its current status (e.g. processing level, quality data) and the past and future (desired end state) of the object.

Using modern identification techniques, production systems can now be realised which can produce variants of a product, or even different products, down to a batch size of one. The automotive industry is a good example: since vehicles are predominantly produces to order and it is rare for two identical vehicles to be ordered, automatic material flow tracking is crucial to smooth operation. A vehicle must be clearly identified at the individual manufacturing stages to avoid, for example, an unwanted are conditioning system from being fitted, or the wrong paint colour being applied during painting.

RFID systems also offer the durability essential for permanent identification of captive product carriers such as:
- Tote boxes, containers, barrels, tubs, and pallets;
- Tool carriers, monorail and power, and free conveyor trolleys;
- Lift trucks, towline carts, automatic guided vehicles.

b. Inventory control
Smart tags are used in warehouses to track inventory. They allow companies to virtually immediately know the location of any item in the warehouse, as well as track boxes as they enter or leave the building.

11.2.3 SECURITY AND ACCESS CONTROL

a. Airport Security
Extremely dense traffic of vehicles, people and goods, combined with high security requirements and timing with aeroplanes make low frequency, short-range RFID solutions unfeasible.

When parcel trams need to urgently pass through doors to the runway area, a high-frequency personnel tag on the driver and readers at the gate make extremely efficient access control possible.

When waiters serving both the airside and landside restaurants from the same kitchen need to conveniently pass through doors with their trays, a hands free system with a tag under the clothes and readers in the ceiling makes it possible to keep the doors locked. No violators can slip through the kitchen between airside and landside.

Utility vehicles passing between different security zones want fast access, and need to be registered for security. Tags on the vehicles and readers at the barriers/gates permits quick, yet secure access control. Extra security is obtained if the RFID system can read and verify grouped tags, where a driver tag and a vehicle tag are used next to each other.

b. Electronic immobilization
In an electronic immobilization system a mechanical ignition key is combined with a transponder. The miniature transponder with a ferrite antenna is incorporated directly into the top of the key. The antenna is integrated into the ignition lock.

The reader antenna is integrated into the ignition lock in such a manner that when the ignition key is inserted, the (inductive) coupling between reader antenna and transponder coil is optimised. The transponder is supplied with energy via the inductive coupling and is therefore totally maintenance free. Electronic immobilisers typically operate at a transmission frequency in the LF range 100 – 135 kHz. ASK modulation is the preferred modulation procedure for the data transfer to the transponder, because it allows the reader and transponder to be manufactured very cheaply. Load modulation is the only procedure used for data transmission from the transponder to the reader.

When the ignition key is turned in the ignition lock to start the vehicle, the reader is activated and data is exchanged with the transponder in the ignition key. Three procedures are employed to check the authenticity of the key:

1. *Checking of an individual serial number.* In almost all transponder systems the transponder has a simple individual serial number (unique number). Very simple systems (first generation immobilization) read the transponder's serial number and compare this with a reference number stored in the reader. If the two numbers are identical the motor electronics are released. The problem here is the fact that the transponder serial number is not protected against unauthorised reading and, in theory, this serial number could be read by an attacker and copied to a special transponder with a writable serial number.

2. *Rolling code procedure*. Every time the key is operated a new number is written to the key transponder's memory. This number is generated by a pseudo-random generator located in the vehicle reader. It is therefore impossible to duplicate the transponder if this system is used.
3. *Cryptographic procedures (authentication) with fixed keys*. The use of cryptographic procedures offers much greater security (second generation immobilization). In vehicle applications, however, unilateral authentication of the key transponder by the reader in the ignition lick is sufficient.

The RFID reader now communicates with the vehicle's motor electronics, although this communication is protected by cryptographic procedures. The motor electronics control all important vehicle functions, in particular the ignition system and the fuel system. Simply short-circuiting of disconnecting certain cables and wires is no longer sufficient to circumvent an electronic immobilization system. Even attempting to fool the motor electronics by inserting another ignition key of the same type into the ignition lock is bound to fail because of the authentication procedure between reader and motor electronics. Only the vehicle's key has the correct (binary) key to successfully complete the authentication sequence with the motor electronics.

c. Checkpoint Systems
Checkpoint's RF technology is a standard for source tagging. It is used for product tagging so that security component is invisible to the consumer.

RF technology is used by all types of retailers, including supermarkets, mass merchandisers, apparel stores, department stores, drug stores, sporting goods stores, automotive stores, and hardware stores for theft protection.

d. Automated Library Systems
Integration of RFID technology into information systems comes from outside traditional supply chain disciplines. RFID technology has found a home in the nation's libraries. This integration speeds up the processing of library materials by providing a swift one step motion for issuing books, eliminating the need to locate and scan a barcode.

Simultaneously, the library's circulation system is automatically updated, and the security is disabled in the software.

It allows for automated checkout and check-in, patron self checkout, built-in security, circulation management, and highly efficient inventory, all integrated into one system.

11.2.4 ANIMAL IDENTIFICATION

Electronic identification systems have been used in stock keeping for almost 20 years and are now state of the art in Europe. In addition to internal application for automatic feeding and calculating productivity, these systems can also be used in inter-company identification, for the control of epidemics and quality assurance and for tracing the

origin of animals. To identify the animal and to store or retrieve information about it, handlers only need to "scan" the animal with a handheld device within a distance of about 3 ft. The required unified data transmission and coding procedures are provided by the 1996 ISO standards 11784 and 11785.

There are four basic procedures for attaching the transponder to the animal: collar transponders, ear tag transponders, injectible transponders and the so-called bolus (***figure 11.1***).

- *Collar transponders* can be easily transferred from one animal to another. This permits the use of this system within a company. Possible applications are automatic feeding in a feeding stall and measuring milk output.
- *Ear tags* incorporating an RFID transponder compete with the much cheaper barcode ear tags. However, the latter are not suitable for total automation, because barcode ear tags must be passed a few centimetres from a hand reader to identify the animal. RFID ear tags, on the other hand, can be read at a distance of up to 1 m.

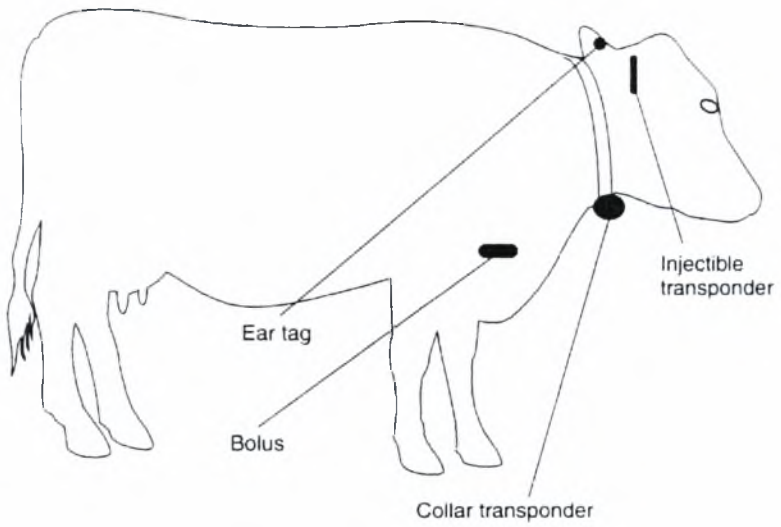

Figure 11.1: The options for attaching the transponder to a cow.

- *Injectible transponders* were first used around 10 years ago. In this system, the transponder is placed under the animal's skin using a special tool. A fixed connection is thereby made between the animal's body and the transponder, which can only be removed by an operation. This allows the use of implants in inter-company applications such as the verification of origin and the control of epidemics. The implant is in the form of a glass transponder of 10, 20 or 30 mm in length. The transponder is supplied in a sterile package or with a dose of disinfectant.
- The so-called *bolus* is a very useful method of fitting the transponder. The bolus is a transponder mounted in an acid resistant, cylindrical housing, which may be made of a ceramic material. The bolus is deposited in the rumen, the omasum that is present on all ruminants, via the gullet using a sensor. Under normal circumstances the bolus remains in the stomach for the animal's entire lifetime. A particular advantage of this

method is the fact that it does not cause any injury to the animal. The removal of the bolus in the slaughterhouse is also simpler than the location and removal of an injected transponder.

11.2.5 MEDICAL APPLICATIONS

a. Disease prevention/cure
The ability of passive transponders to operate reliably for years without their own power supply – which may be susceptible to failure – predestined this technology for applications in human medicine.

Glaucoma is a condition in which increased interocular pressure (IOP) at first causes a narrowing of the field of vision, and ultimately results in complete blindness. The latest research has shown that interocular pressure is subject to sharp diurnal fluctuations and that not only the absolute pressure, but also the pressure fluctuations, significantly influence the risk of blindness. Therefore, the continuous measurement of the niterocular pressure under normal conditions and in the patient's normal environment is necessary to improve understanding of the progression of the condition and facilitate an individual programme of treatment. This is in contrast to the normal practice of measuring IOP exclusively during surgery hours with the aid of a tonometer.

In patients with a cataract, the natural lens is removed from the eye and replaced by an artificial interocular lens. This prompted the idea of integrating a full transponder, i.e. a microcoil and a transponder chip with an integral capacitive pressure sensor, into the haptic of such an artificial intraocular lens. So that the transponder can be read continuously, the reader's antenna is integrated into the frame of a pair of glasses. The control of the coil and the storage of the measured data take place with the aid of the reader, which is connected to the glasses via a cable.

b. Healthcare
The healthcare industry is beginning to use RFID labels and tags to track supplies and pharmaceuticals, including their expiration dates, as well as portable diagnostic equipment shared between departments. These enables healthcare institutions to better control inventory and maximize their equipment to keep costs down, while delivering the highest level of patient care.

11.2.6 SPORTING EVENTS

In large-scale sporting events such as major marathons, the runners who start at the back of the field are always at a disadvantage, because their times are calculated from the moment the race is started. For many runners it takes several minutes before they actually cross the starting line. In very large events with 10.000 participants or more, it might be 5

minutes before the last runners have crossed the starting line. Without individual timing, the runners in the back rows are therefore at a severe disadvantage.

To rectify this injustice, all runners carry a transponder with them. The system is based upon the idea that each runner places his feet repeatedly on the found and thus comes very close to a ground antenna. In experimental events it was found that using an ingenious arrangement of multiple antennas in an array and a chip in the shoe over 1000 runners can be registered up to eight times in a minute with a start width of just 4m.

12. Historical Barriers To RFID Adoption

While RFID has been commercially available for over two decades, the rate of adoption for most applications has been slow as the relative benefits of the technology have been outweighed by several key barriers, including lack of standards, relatively high cost, weak education, technology hurdles and privacy concerns. As a result, RFID has historically been used in only niche applications. The following factors describe the key barriers that have kept RFID from becoming more widespread.

- **Lack of Standards**
  Current industry RFID standards are largely incomplete with respect to addressing a number of technology and application issues. RFID has been implemented in different ways by different manufacturers and global standards are still being worked on. The lack of standards has kept many potential users from investing in RFID for fear that supply chain partners may use incompatible RFID products, or that future standards may obsolete current RFID formats. By contrast, bar coding has been widely adopted over the past 25 years with its high degree of standardization.
- **Relatively High Cost / Infrastructure**
  RFID's robust functionality can easily lead to significant improvements in supply chain operations; however, the overall system cost is a key reason why this enhanced functionality remains under-used. A low-end passive RFID tag costs approximately $0.25-$0.50, with high-end active tags reaching up to $250 each. That compares to less than $0.01 for a bar code label. In addition, RFID requires new infrastructure, where RFID readers can cost $1,200-$3,500 each. Further, RFID solutions often involve a challenging front-end integration process. As a result, many end users have found it difficult to justify the cost of an RFID system despite the apparent incremental benefits. A.T. Kearney has calculated that initial RFID tagging infrastructure costs of $400,000 will be required per distribution center, and $100,000 will be required per store. In addition, AMR published a study concluding that the initial integration charges for an RFID supply chain tracking application could be as much as $15M-$20M for a company that ships 50 million tagged cases per year.
- **Lack of Education**
  The majority of potential RFID users lack a clear understanding of the potential RFID benefits, instead they remain weary of RFID's relatively high cost. In addition, many end users view implementation of a new technology as a daunting task.
- **Technology Hurdles**
  A finding of AMR research indicated that RFID read rates are approximately 80%. A substantial percentage of the failure comes from a poor connection between the chip and the antenna on the transponder, which is generally caused by underdeveloped manufacturing processes. In addition, a portion of the high failure rate can be attributed to environment, such as the presence of metals, liquids (UHF products have difficulty reading through liquids) or other RF energy. It is expected that end users will require read rates approaching 100% before considering a significant implementation of RFID.
- **Privacy Concerns**
  Privacy groups have expressed a concern that RFID, due to its small form factor and RF attributes, will allow monitoring of individuals' behavior without their

knowledge. Several opponents to RFID have organized, including Consumers against Supermarket Privacy Invasion and Numbering, or CASPIAN to derail adoption of the technology. As a result, several retail pilots, including Benetton, have been canceled.

- **Volume of Data**
  The data volume generated by RFID could be sizeable since RFID tags can carry orders of magnitude more data than a typical bar code.

13. Medium Access Control protocol for reader singulation

13.1 Introduction

In RFID systems, an RFID reader may interfere with the operation of other readers in the system. Interference caused by the operation of an RFID reader is referred to as a reader collision. Reader collisions prevent the colliding readers from communicating with the RFID tags in their respective reading zones. Therefore, reader collisions must be avoided whenever possible to ensure proper and timely communication with tags. The task of preventing reader collisions is referred to as the ***reader collision problem***.

In this chapter, we are concerned with RFID systems where many tags and many readers exist, such as supply chain management applications (store shelf scanning, warehouse shelf management, general pallet identification, passage of goods through warehouse docking doors, etc.) or futuristic systems where every object bears a tag (e.g the reader embedded in the microwave oven reads the tag attached to the food packet). Specifically, we are concerned with efficient Medium Access Control protocols that could be occupied to synchronize the readers of the system in order to solve the reader collision problem.

In order to find a proper Medium Access Control protocol for each application, the following factors should be taken into account:

- ***How many*** tags should be singulated
  - All
  - Group
  - Single
- ***How often***
  - Once
  - Constantly
  - Periodically/occasionally
- ***Reader mobility***
- ***Tag distribution***

Some scenarios encountered in supply chain management as well as their characteristics as far as medium access control is concerned are the following:

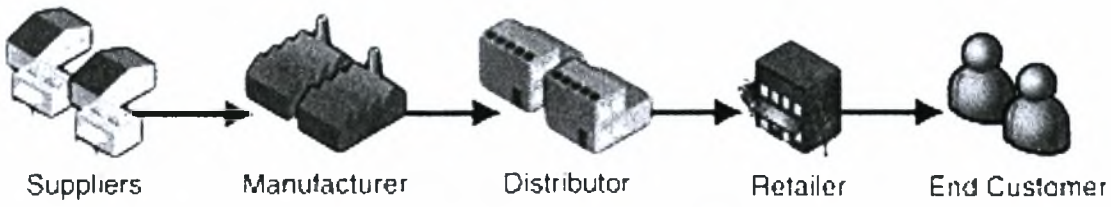

Figure 13.1: The supply chain.

- 1 reader in an entry/exit door – readers in sequential entry/exit doors
  - Receiving, Shipping (receiving and shipping of products in cases/palettes):
    - Scanning in palette/case level all cases/palettes (case/palette EPCs should have a common prefix; different from that of item EPCs)
    - Scanning once
  - Checkout (while exiting a store, the client is charged for the products he bought):
    - Scanning in item-level all items
    - Scanning once

- Handheld readers (scan palettes further upon receiving, find specific items, e.g. misplaced items)
  - Single tag, constant scanning
  - Reader mobility

- Readers in forklifts (palette/case/product transfer to the correct storage area (e.g.shelf)/assembly line)
  - All tags, constant scanning
  - Reader mobility

- Readers in each machine used in a factory
  - All tags, occasional scanning (scanning while not occupied, but constant scanning when scanning),

- Readers adjacent to conveyor belts (routing of cases/palettes/products)
  - All tags, constant scanning

- Readers on the shelves of a warehouse/store ((almost) real-time product visibility)
  - All tags/ Group(products from a specific manufacturer)/ Single(product existence verification) singulation
  - Constant (products with a rapidly changing quantity, e.g. batteries) or periodical (products with a less rapidly changing quantity, e.g. TVs) scanning.
  - Uniform / Not uniform tag distribution

- Readers in the yard (for products sitting in the yard, but not officially received yet)
  - All tags scanning
  - Periodic

- Readers within a transportation truck (case/palette/product scanning mainly for security reasons)
  - All tags scanning
  - Periodic

As far as futuristic systems are concerned, the following approaches could be followed:

- Reader in each entry/exit; these readers must scan constantly

- Readers on shelves; frequently used items should be scanned constantly (e.g. any item lies on the office desk), less frequently used items could be scanned periodically (e.g. old books in a library).
- Readers-sentinels to singulate readers that function occasionally
  - e.g. the reader in the microwave oven sends an RTS and after getting permission from the sentinel (which forces some other readers to temporarily pause) communicates with the food packet

13.2 Application Simulation

In the following sections, a Medium Access Control protocol for the ***store shelf scanning*** application is considered. The RFID system used is shown in the following picture:

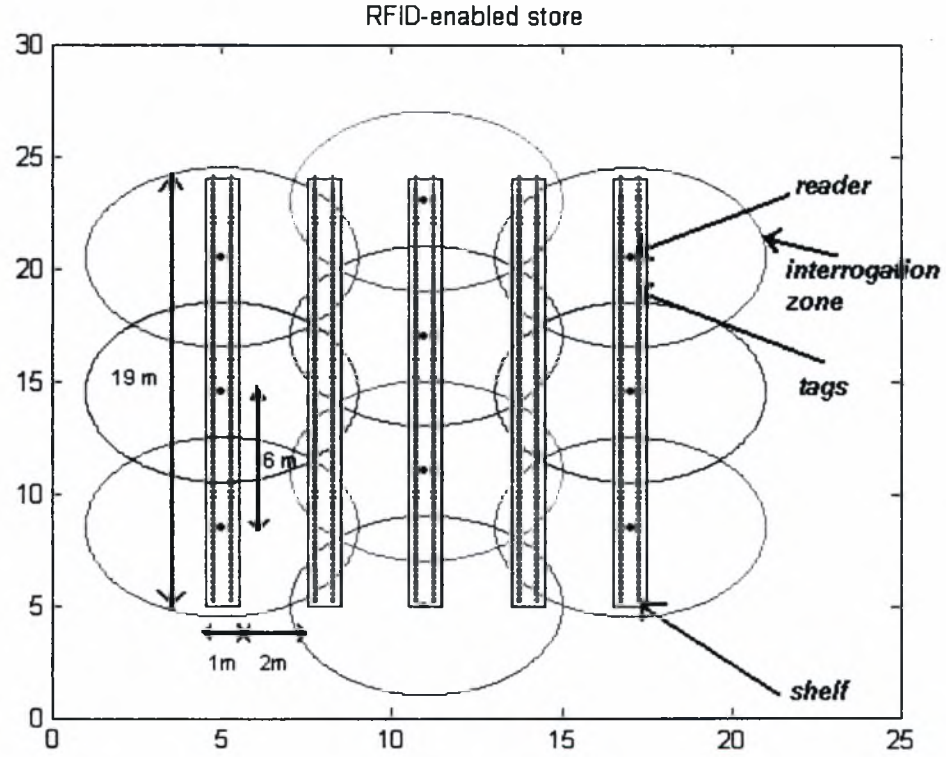

Figure 13.2: Network topology for the store shelf scanning application.

The protocol initially realized and refined later is a centralized protocol (the scheduling decisions are made by the application software) that achieves reader singulation using TDMA, where:

- Each reader is assigned 1 timeslot per frame, based on the slots already assigned to its neighbours (neighbour readers should not transmit at the same time).
- In each slot, more than one reader is allowed to transmit.

In the following sections, we will refer to that protocol as the TDMA protocol.

13.2.1 Simulation Details

1. The RFID system operates in the UHF ISM frequency band.
2. The tags used are EPC Class 0 tags (backscatter, passive, read-only). The reasons for such a choice are the following:
   - read-only memory technologies enable miniaturization
   - standards for superior classes than class 0 and class 1 tags are still in progress
   - read-write tags are useful in some specialized applications, but since they are more expensive than read-only chips, they are impractical for tracking inexpensive items.
3. The reader's interrogation zone is realized as a circle of radius 4.2 m.
4. Propagation and processing delays are negligible
5. The anticollision method used is the tree-walking protocol as defined in the EPC standard for Class0 tags operating in the UHF range. In each tree traversal, the whole population of tags is addressed (not a specific group or tag).
6. ***Duplicate IDs issue***
   - From the spec, every tag has an internal ID flag stating whether is has been read or not.
7. ***Frequency Hopping***
   - Each reader chooses a new frequency every 400ms of transmission; the exact frequency is not defined, but it doesn't matter since neighbor readers do not transmit at the same time.
   - In each frequency hopping, Reset must be performed; we adopt the approach that Reset doesn't influence the state of the tags' internal ID flag (so we must not start the tree traversal from the beginning).
8. We assume that each reader is assigned 1 large timeslot (multiple of the 400 msec period)

13.2.2 Results

Initial experiments:

Since the tag population in applications as store shelf scanning is expected to be high, the protocols employed (both for anticollision and reader singulation) should ensure that the tags addressed can be read in time.

1. Increasing the number of tags per shelf, we have the following results.

Number of readers	10	10	10
Number of tags per shelf	240	510	840
Total number of tags	1200	2550	4200

Reader range (m)	4.2	4.2	4.2
Timeslot duration (multiple of 400 ms)	400ms	800ms	1200ms
Number of slots in a TDMA frame	4	4	4
Network throughput: tags/msec	0.75	0.79	0.87

Figure 13.3: Performance vs. tag population.

We observe that the network's throughput increases as the tag population that can be addressed in a predetermined timeslot increases. However, since the time measured is based on timeslots, if the number of tags addressed by a reader exceeds the number of tags that can be addressed in the predetermined timeslot, the timeslot duration will increase and the network's throughput will decrease.

2. Increasing the density of the readers (by decreasing the distance between the shelves), we have the following results.

Number of readers	10	10	10
Number of tags per shelf	510	510	510
Total number of tags	2550	2550	2550
Reader range (m)	4.2	4.2	4.2
Distance between shelves	2m	1.5m	1.1m
Timeslot duration (multiple of 400 ms)	800ms	800ms	1200ms
Number of slots in a TDMA frame	4	4	4
Network throughput: tags/msec	0.79	0.79	0.53

Figure 13.4: Performance vs. reader density.

We observe that the readers' density increase may cause a decrease in the network's throughput. It happens when either the neighbors of the readers are increased (the number of colliding readers increases and thus we need more timeslots to scan all the products) or the number of tags that a reader addresses in a predetermined timeslot is increased since

the common areas between two readers are increased (thus the timeslot duration must be increased).

Issues to consider:

1. Non-uniform tag distribution

Since not all the products found in a store have the same dimensions (e.g. a shelf with radios and a shelf with batteries), it would be rather unrealistic to assume that the tag distribution over the readers is uniform. Instead, extending the protocol mentioned above, the following approaches have been proposed in order to maximize the throughput of a system (number of tags read per time unit) with non-uniform tag distribution:

1. The same number of timeslots is assigned to each reader, but
   a) Readers are scheduled in such a way that tags being in the range of 2 readers are read by the reader with the smallest number of tags.
   b) Readers with many tags reduce their range, readers with a few tags increase their range – the application software should ensure that no tag is out of range. (The range of each of the 3 most powerful readers in the network (the readers with the greatest number of tags in their interrogation zone) is reduced by 0.2m and the range of at least one of their neighbors – until no tag is out of range – is increased by 0.2m. The neighbors chosen to increase their range are the neighbor readers with the least number of tags in their interrogation zone)
2. Different number of timeslots is assigned to each reader according to the number of tags in its interrogation zone.

As we can see from the following table, for the network topology given above, all the three approaches lead to an increased throughput.

	TDMA	1a	1b	2
Number of readers	10	10	10	10
Number of tags per shelf	450	450	450	450
Total number of tags	2250	2250	2250	2250
Reader range (m)	4.2	4.2	Variable (initial: 4.2)	4.2
Timeslot duration (multiple of 400 ms)	1200ms	800ms	800ms	400ms
Number of slots in a TDMA frame	4	4	4	7
Network throughput: tags/msec	0.469	0.703	0.703	0.8

Figure 13.5: Performance in non-uniform tag distribution.

Which approach is the best depends on the network topology. Thus,

- Approach (1a) is the simplest method of those mentioned and works especially well when the difference in the tag population between neighboring readers is small.

- Approach (1b) works well when the difference in the tag population between neighboring readers is small, too. We can obtain especially good results when there is 1 reader with a small number of tags surrounded by readers with many tags or when there is a reader with many tags surrounded by readers with a small number of tags.
- Approach (2) works well in any network topology. However, it is the most complicated method, since the number of tags in each reader should be checked regularly in order to assign the correct number of timeslots to each reader.

2. Reduced number of readers – access based on certain QoS constraints

Sometimes, the number of readers is not sufficient to cover all the tags. Instead of adding more readers, some of the existing readers could move periodically from one position to another in order to read the tags that were initially out of range. This causes some tags to be "periodically scanned" (period = the time until the moving reader returns to its initial position). In fact, it is not a problem when the products that are to be periodically scanned are products that are not consumed very often or in large quantities. E.g. a store could sell many batteries all over the day, but only a few televisions. Thus, the quantity of batteries should be checked regularly, while the quantity of televisions could be scanned periodically. In other words, for each product of the store, some QoS constraints should be defined for the interval between two consecutive accesses of the same product.

The approaches considered to synchronize periodically and constantly scanning readers are the following:
(1) Every x TDMA frames considering only constant scanning readers, a frame considering ***only*** the periodically scanning readers is interleaved
(2) Every x TDMA frames considering only constant scanning readers, a frame considering ***both*** constantly and periodically scanning readers is interleaved

The simulation pattern followed is described below:
- 1 TDMA frame considering only the periodically scanning readers in their *initial position* (1) or the periodically scanning readers in their initial position and the constantly scanning readers (2)
- x TDMA frames considering only the constant scanning readers
- 1 TDMA frame considering only the periodically scanning readers in their *final position* (1) or the periodically scanning readers in their final position and the constantly scanning readers (2)
- x TDMA frames considering only the constant scanning readers

The interval between two consecutive accesses of the same product (for products scanned periodically) is 2*x TDMA frames (for the immobile readers) + 1 TDMA frame (periodically scanning readers in their initial position) + 1 TDMA frame (periodically scanning readers in their final position). This interval should not be greater than the maximum interval defined by the QoS constraints.

As we can see from the following table, although the number of the network readers is not sufficient to cover all the tags, the throughput of the RFID system can increase, depending upon the location of the moving readers. The 2nd approach provides better throughput, but the maximum interval between two consecutive accesses of the same tag increases.

	TDMA	1	2
Number of readers	10	10	10
Number of tags per shelf	450	450	450
Total number of tags	2250	2250	2250
Reader range (m)	4.2	4.2	4.2
x parameter		3	3
Number of moving readers	0	1	1
Timeslot duration (multiple of 400 ms)	1200ms	800ms (periodical scanning), 1200ms (constant scanning)	1200ms
Number of slots in a TDMA frame	4	1 (periodical scanning), 3 (constant scanning)	3
Total number of simulation TDMA frames	8	8	8
Network throughput: tags/msec	0.469	0.535	0.557
Max Interval between 2 consecutive accesses of the same tag (sec)	4,8	23.2 (periodical scanning), 4.4 (constant scanning)	28.8 (periodical scanning), 7.2 (constant scanning)

Figure 13.6: Performance when the number of readers is reduced.

3. Immobile and mobile readers

In a store shelf scanning RFID system, apart from the shelves' readers, mobile readers may be used. E.g. if a bottle of milk expires, a handheld reader will try to locate this bottle by querying for the identification number of its tag and possibly colliding with the shelves' readers. Thus, the system should handle mobile readers, too. The approaches considered are the following:

(1) The shelves' readers stop communication with tags for the current TDMA slot when they sense a collision with another reader (the handheld reader); a secure environment is assumed.

(2) The handheld reader requests from the application software to transmit and waits until it is notified to begin transmission. The application software gives permission for transmission to the handheld reader when the current TDMA frame ends. After the handheld reader has ended transmission, it notifies the application software, which

commands the shelves' readers to continue transmitting according to the TDMA procedure.

To simulate the case of immobile and mobile readers, the following simulation pattern was used:
- 1 TDMA frame for the immobile readers
- 1 TDMA frame (in case (2), much smaller than a normal TDMA frame) during which the handheld reader transmits
- 1 TDMA frame for the immobile readers

Since the arrival time of the handheld reader as well as whether the handheld reader collides with an immobile reader are not deterministic, an average case was attempted by using the above simulation pattern for 15 iterations.

Assuming that the handheld reader makes 5 queries until it determines the exact position of the requested tag, the following results are produced.

	TDMA	1	2
Number of readers	10	10	10
Number of tags per shelf	450	450	450
Total number of tags	2250	2250	2250
Reader range (m)	4.2	4.2	4.2
Timeslot duration (multiple of 400 ms)	1200ms	1200ms	1200ms
Number of slots in a TDMA frame	4	4	4
Network throughput: tags/msec	0.469	0.466	0.469
Average same tag reading interval	4.8 sec	5.76 sec	4.81 sec
Mean time in system (for the handheld reader)		10.4 ms	1.92 sec

Figure 13.7: Performance in the presence of mobile readers.

As we can see from the above table, using the 2nd approach, the network's throughput remains the same as in TDMA, while the interval between two consecutive accesses of the same tag increases slightly. Using the 1st approach, the network's throughput is decreased slightly and the average interval between two consecutive accesses of the same tag increases by almost 25% of the initial value in TDMA (in fact by 1/number of slots per frame). The mean time of the handheld reader in the system is much greater in the 2nd approach than in the 1st one.

To sum up, both approaches provide almost the same throughput as TDMA. Using the 1st approach, the requested tag can be found much more quickly than using the 2nd approach;

however, the 1st approach demands higher values for the maximum time between two consecutive accesses of the same tag (not strict QoS constraints).

14. RFID Terms

Active Tags Tags that use batteries as a partial or complete source of power. They are further differentiated by separating them into those with replaceable batteries and those which have the batteries inside a sealed unit or what may be termed unitized active tags.

Antenna - Antennas are the conductive elements that radiate, and/or receive energy in the radio frequency spectrum, to and from the tag.

Bidirectional - Capable of operating in either of two directions which are the opposite of each other. For example, a tag, which can be read or written, from either side is bi-directional.

Capacity - The number of bits or bytes that can be programmed into a tag. This may represent the bits accessible to the user or the total number including those reserved to the manufacturer e.g. parity or control bits.

Electromagnetic Coupling - Systems that use a magnetic field as a means of transferring data or power are said to use electromagnetic coupling.

Electronic Label - Label that has an electronic RFID tag embedded within.

Electrostatic coupling - Systems that use the inducing of a voltage on a plate as a means of transferring data or power are said to use electrostatic coupling.

Error Correcting Code (ECC) - Supplemental bits in a data transfer used in conjunction with a polynomial algorithm, in order to compute the value of missing or erroneous data bits (e.g. for a 32 bit data transmission, 7 additional bits are required.)

Error Rate - The number of errors per number of transactions.

Factory Programming - The programming of information into a tag occurring as part of the manufacturing process resulting in a read only tag.

Field Programming - Programming information into the tags may occur after the tag has been shipped from the manufacturer to an OEM customer or end user or in some cases to the manufacturer's distribution locations. Field programming usually occurs before the tag is installed on the object to be identified. This approach enables the introduction of data relevant to the specifics of the application into the tag at any time; however, the tag would typically have to be removed from its object. In some cases, change or duplication of all data in the tag is possible. In other cases, some portion is reserved for factory programming. This might include a unique tag serial number, for example.

Field Protection - The ability to limit the operations which can be performed on portions or fields of the data stored in a tag.

Frequency - The number of times a signal executes a complete excursion through its maximum and minimum values and returns to the same value (e.g. cycles).

Inductive Coupling - Systems that use the inducing of a current in a coil as a means of transferring data or power are said to use inductive coupling.

In Use Programming - Many applications require that new data or revisions to data already in the tag, be entered into the tag, while it remains attached to its object. The ability to read from and write data to the tag while attached to its object is called in-use programming. Tags and systems with this capability are called read/write tags and systems.

Life - Functional period within which no maintenance, adjustment or repair is to be reasonably expected.

Memory Cards - A read/write or reprogrammable tag in credit card size

Memory Modules - A read/write or reprogrammable tag

Misread - A condition that exists when the data presented by the reader is different from the corresponding data in the tag.

Modulation - The methods of modulating or altering the carriers in order to carry the encoded information are quite varied. They include amplitude modulation (AM)/ phase modulation (PM), frequency modulation (FM), frequency shift keyed (FSK), pulse position (PPM), pulse duration (PDM) and continuous wave (CW). In some cases, different modulating techniques are used in each direction (to and from the tags).

Modulation, amplitude (AM) - Data is contained in changes in amplitude of the carrier.

Nominal - The value at which a system is designed to assure optimal operation. Tolerance considers the "normal" deviation of variable factors.

Nominal Range - The range at which a system can assure reliable operation, considering the normal variability of the environment in which it is used.

Omnidirectional - Capability of a tag to operate in any orientation.

Passive Tags - Passive tags contain no internal power source. They are externally powered and typically derive their power from the carrier signal radiated from the scanner.

Power Levels - Levels of power radiated from a scanner or tag, usually measured in volts/meter.

Programming - Adding or altering in a tag.

RFID - Systems that read or write data to RF tags that are present in a radio frequency field projected from RF reading/writing equipment. Data may be contained in one or more bits for the purpose of providing identification and other information relevant to the object to which the tag is attached. It incorporates the use of electromagnetic or electrostatic coupling in the radio

Write Rate - The rate at which information is transferred to a tag, written into the tag's memory and verified as being correct. It is quantified as the average number of bits or bytes per second in which the complete transaction can be performed.

Bibliography

[1] Klaus Finkenzeller, "RFID-Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification", Wiley & Sons LTD, 2nd Edition (April 2003)

[2] Interaction Design Institute Ivrea - Harnessing Technology Project, "RFID: a week long survey on the technology and its potential", March 2002

[3] CAEN(http://www.caen.it), Application Note: "Introduction to RFID Technology"

[4] Pete Sorrells, Microchip Technology Inc., "Passive RFID Basics", 1998

[5] Rakesh Kumar (Wipro Technologies, India), "Interaction of RFID Technology and Public Policy", Paper presentation at RFID Privacy Workshop @ MIT, Massachusetts, 2003

[6] Micah Sherr, Presentation: "RFID tags", January 16th, 2004

[7] Craig K. Harmon, Presentation: "Basics of RFID Technology", 16 September 2003

[8] Robert W. Baird & Co., "RFID Explained – A basic overview", February 2004

[9] Roy Want, Intel Research, "Enabling Ubiquitous Sensing with RFID", Invisible Computing, April 2004

[10] Bob Scher, Dynasys Technologies Inc., "What is Radio Frequency Identification?", 2004

[11] Bob Scher, Dynasys Technologies Inc., "Everything you wanted to know about transponder types but were afraid to ask", 2004

[12] Susy d'Hont, Texas Instrument TIRIS, "The Cutting Edge of RFID Technology and Applications for Manufacturing and Distribution"

[13] ACSIS Inc., "Lessons from the Front Line – RFID Integration"

[14] Tektronix Inc. (www.tektronix.com), Technical Brief: "Radio Frequency Identification (RFID) Overview"

[15] IDTechEx (http://www.idtechex.com/) White Paper, "RFID Explained – An introduction to RFID and tagging technologies", 2004

[16] "RFID Tags And Chips: Changing The World For Less Than The Price Of A Cup Of Coffee", In-Stat, December 2004

[17] Bob Scher, Dynasys Technologies Inc., "Understanding RFID frequencies", 2004

[18] Philips Semiconductors, TAGSYS, Texas Instruments Inc., "Item-Level visibility in the pharmaceutical supply chain: A comparison of HF and UHF RFID technologies", July 2004

[19] Leonid Bolotnyy, Presentation: "RFID Privacy", February 24, 2004

[20] Simson Garfinkel, "An RFID Bill of Rights", Technology Review, page 35, October 2002

[21] http://www.autoid.org/, White Paper: "Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility", 2002

[22] Yun Kang, Stanley Gershwin, "Information Inaccuracy in Inventory Systems – Stock Loss and Stockout", August 23, 2004

[23] Kui Mok, Alvin Lim, "Wireless Media Access Control for High Mobile Inforamtion Servers: Simulation and Performance Evaluation", Mobile Computing and Communications Review, Volume 1, Number 2

[24] Ari Juels, Ronald Rivest, Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", pp. 103-111, ACM Press, 2003

[25] Imrich Chlamtac, Chiara Petrioli, Jason Redi, "Energy-Conserving Access Protocols for Identification Networks", IEEE/ACM Transactions on Networking, Vol. 7, No. 1, February 1999
[26] Milan Nosovic, Terence D. Todd, "Scheduled rendezvous and RFID wakeup in embedded wireless networks", ICC 2002 - IEEE International Conference on Communications, vol. 25, no. 1, pp. 3325-3329, April 2002
[27] Transponder News (http://rapidttp.com/transponder)
[28] RFID Journal (http://www.rfidjournal.com/)
[29] Articles about RFID, Technovelgy.com (http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=2)
[30] http://www.rfidusa.com/
[31] http://rfid-active.com
[32] RFID Survival (http://www.rfidsurvival.com/)